Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-206335
Filing date: 13 July 2004 (13.07.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年　７月１３日
出 願 番 号 Application Number:	特願２００４－２０６３３５
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２０６３３５
出 願 人 Applicant(s):	松下電器産業株式会社

２００５年　４月１３日

特許庁長官
Commissioner,
Japan Patent Office

小 川

【書類名】　特許願
【整理番号】　2048160240
【提出日】　平成16年 7月13日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　宮崎　雅也
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　雅哉
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　村瀬　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　小野田　仙一
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを受け付ける入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項２】
コンテンツを実行、もしくは再生する実行装置であって、
前記実行装置は、
認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、
を備えることを特徴とする実行装置。
【請求項３】
前記取得部は、可搬媒体からデータを取得すること、
を特徴とする、請求項２に記載の実行装置。
【請求項４】
前記可搬媒体は光ディスクであり、
前記取得部は、前記光ディスク経由でデータを取得し、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、
を特徴とする、請求項３に記載の実行装置。
【請求項５】
前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、

を特徴とする、請求項４に記載の実行装置。
【請求項６】
前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、
を特徴とする、請求項２に記載の実行装置。
【請求項７】
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、
を特徴とする、請求項２から請求項６のいずれか１項に記載の実行装置。
【請求項８】
前記実行装置は、さらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、を備え、
前記取得部は、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信し、
前記実行部は、前記暗号化コンテンツを復号化すること、
を特徴とする、請求項２から請求項７のいずれか１項に記載の実行装置。
【請求項９】
前記実行装置は、さらに、
デバイス鍵を保持するデバイス鍵格納部と、
前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、
前記取得部はさらに、前記暗号化鍵束を受信すること、
を特徴とする、請求項８に記載の実行装置。
【請求項１０】
前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする、請求項２から請求項９のいずれか１項に記載の実行装置。
【請求項１１】
前記検証情報は、デジタル署名方式の検証鍵であること、
を特徴とする、請求項２から請求項１０のいずれか１項に記載の実行装置。
【請求項１２】
前記認証情報検証部は、前記検証情報及び前記コンテンツの属性値及び前記配布データ領域特定情報を基に、認証情報を検証すること、
を特徴とする、請求項２から請求項１１のいずれか１項に記載の実行装置。
【請求項１３】
前記取得部は、さらに、前記コンテンツの属性値を取得すること、
を特徴とする、請求項１２に記載の実行装置。
【請求項１４】
前記コンテンツは、前記実行装置で実行可能なプログラムであり、
前記実行部は、前記プログラムを実行すること、
を特徴とする請求項２から請求項１３のいずれか１項に記載の実行装置。
【請求項１５】
コンテンツを配布する配布センタであって、
前記配布センタは、
前記コンテンツを受け付ける入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布

する配布部と、を備え、
を備えることを特徴とする配布センタ。
【請求項１６】
前記配布部は、可搬媒体へデータを記録すること、
を特徴とする、請求項１５に記載の配布センタ。
【請求項１７】
前記可搬媒体は光ディスクであり、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、
を特徴とする、請求項１６に記載の配布センタ。
【請求項１８】
前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、
を特徴とする、請求項１７に記載の配布センタ。
【請求項１９】
前記配布部は、記録媒体、もしくは通信ネットワーク、もしくは放送網を介してデータを配布すること、
を特徴とする、請求項１５に記載の実行装置。
【請求項２０】
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、
を特徴とする、請求項１５から請求項１９のいずれか１項に記載の実行装置。
【請求項２１】
前記配布センタはさらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する暗号化部と、を備え、
前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、
を特徴とする、請求項１５から請求項２０のいずれか１項に記載の配布センタ。
【請求項２２】
前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする、請求項２１に記載の配布センタ。
【請求項２３】
前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする、請求項１５から請求項２２のいずれか１項に記載の配布センタ。
【請求項２４】
前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項１５から請求項２３のいずれか１項に記載の配布センタ。
【請求項２５】
前記認証情報生成部は、認証情報生成情報を基に、前記配布データ領域特定情報及び前記コンテンツの属性値を含む検証対象データに対する認証情報を生成すること、
を特徴とする、請求項１５から請求項２４のいずれか１項に記載の配布センタ。
【請求項２６】
前記配布部は、さらに、前記コンテンツの属性値を配布すること、
を特徴とする、請求項２５に記載の配布センタ。

【請求項２７】
前記コンテンツはプログラムであること、
を特徴とする請求項１５から請求項２６のいずれか１項に記載の配布センタ。
【請求項２８】
不正コンテンツを検知する不正コンテンツ検知方法であって、
前記不正コンテンツ検知方法は、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布手段と、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行手段と、から構成され、
前記配布手段は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、
前記実行手段は、
前記認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする不正コンテンツ検知方法。
【請求項２９】
コンテンツを実行、もしくは再生する実行方法であって、
前記実行方法は、
認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする実行方法。
【請求項３０】
コンテンツを配布する配布方法であって、
前記配布方法は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、

を備えることを特徴とする配布方法。

【書類名】明細書
【発明の名称】不正コンテンツ検知システム
【技術分野】
【０００１】
本発明は不正なコンテンツを検知する技術に関するものである。
【背景技術】
【０００２】
近年、デジタルコンテンツの普及に伴い、例えば著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる不正コンテンツ（違法コンテンツ）の配布が社会問題となってきている。この不正コンテンツ配布の一つのケースとして、映画館等で上映される映画コンテンツを、例えば著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した不正動画コンテンツを光ディスクに記録し販売するというものが挙げられる。また別のケースとして、正規に販売されている片面２層ＤＶＤ－ＲＯＭディスク（最大８．５ギガバイト）に記録されているＤＶＤ－ＶＩＤＥＯ形式の映画コンテンツの画質を４．７ギガバイト以下に収まるように変換処理をして不正コンテンツを生成して、その不正コンテンツを片面１層ＤＶＤ－Ｒディスク（最大４．７ギガバイト）に記録して販売するものも挙げられる。
【０００３】
上記のような不正コンテンツ配布（不正コンテンツ利用）を防ぐ方法の従来技術としては、特許文献１に記載されている不正コンテンツ検知システムと自明な方式が知られている。
特許文献１に記載の従来技術は、可搬媒体の中に、複数のコンテンツブロック（部分コンテンツ）から構成されるコンテンツデータの他に、複数のコンテンツブロックに対応するハッシュ値と、複数のハッシュ値を結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前に、記録されたハッシュ値が正規の著作権者によって記録されたものか、デジタル署名を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生開始をしない。また、コンテンツを再生している途中にも、記録されたハッシュ値がコンテンツデータの正しいハッシュ値なのか検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が不正コンテンツを可搬媒体に記録して配布したとしても、実行装置ではその不正コンテンツを再生開始しないか、途中で再生を停止する。これにより、不正なコンテンツの配布防止につながる。
【０００４】
ここでは、特許文献１に記載の従来技術の詳細の一例について図３５を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。初めに、正規の著作権者が、コンテンツデータと、複数のコンテンツブロックに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツをｎ個（ｎは２以上の自然数）のコンテンツブロック（図３７のコンテンツブロック　ＢＬＫ１・・・ＢＬＫｎに対応）に分割する。そして、一方向性関数を用いてコンテンツブロックＢＬＫ１のハッシュ値ＨＡＳＨ１を計算する。コンテンツブロックＢＬＫ２以降も同様にハッシュ値を計算し、それぞれのコンテンツブロックＢＬＫ２、・・・、ＢＬＫｎに対応するハッシュ値ＨＡＳＨ２、・・・、ＨＡＳＨｎを求める。そして、ｎ個のハッシュ値ＨＡＳＨ１、・・・、ＨＡＳＨｎを連結させたものをヘッダ情報とする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報のデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始す

る。その後、実行装置はコンテンツを再生しながら、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテンツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。このような特許文献１に記載の従来技術により、何らかの理由によりコンテンツが盗み出され、例えば著作権を保持しない者がそのコンテンツを可搬媒体に記録して配布、販売しようとしても、可搬媒体には著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正コンテンツ流通に対する対策が可能となる。

【０００５】

この特許文献１に記載の従来技術の課題は、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという点である。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【０００６】

上記に記載の課題を解決するものとして自明な方式が挙げられる。自明な方式では、可搬媒体の中に、コンテンツデータの他に、そのコンテンツデータに対するデジタル署名を記録しておく。そして、実行装置では、記録されたデジタル署名がコンテンツデータに対する著作権者の正規のデジタル署名であることが検証された場合に、可搬媒体の中のコンテンツを再生する。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを再生しない。これにより、不正なコンテンツの配布防止につながる。

【特許文献１】米国特許第６４８０９６１号明細書
【特許文献２】特開２００２－２８１０１３号公報
【非特許文献１】「情報セキュリティ」宮地充子・菊池浩明編著　情報処理学会編集
【非特許文献２】「ＴＨＥ　ＡＲＴ　ＯＦ　ＣＯＭＰＵＴＥＲ　ＰＲＯＧＲＡＭＭＩＮＧ　Ｖｏｌ．２　～　ＳＥＭＩＮＵＭＥＲＩＣＡＬ　ＡＬＧＯＲＩＴＨＭＳ」　ＤＯＮＡＬＤ　Ｅ．　ＫＮＵＴＨ　著、ＩＳＢＮ　０－２０１－０３８２２－６
【非特許文献３】「Ｐｒｏｔｏｃｏｌｓ　ｆｏｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　Ｋｅｙ　Ｅｓｔａｂｌｉｓｈｍｅｎｔ」　Ｃｏｌｉｎ　Ｂｏｙｄ／Ａｎｉｓｈ　Ｍａｔｈｕｒｉａ著、ＩＳＢＮ　３－５４０－４３１０７－１

【発明の開示】
【発明が解決しようとする課題】

【０００７】

ここでは、不正コンテンツが配布される別の一形態として、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録（追記）されるという不正行為を想定する。また、別の一形態として、著作権を保持しない不正者によって、正規の著作権者により配布された可搬媒体に記録されている全データを別の可搬媒体（前の可搬媒体と同じデータサイズを記録可能な可搬媒体であってもよいし、前の可搬媒体以上のデータサイズを記録可能な可搬媒体であってもよい）にコピーして、その別の可搬媒体で記録可能なデータ領域に不正コンテンツが記録（追記）されるという不正行為も想定する。このような場合、上記で説明した自明な方式における実行装置では、正規の著作権者により記録された認証情報により認証が成功してしまうことで、コンテンツの実行、再生を開始してしまい、最終的には可搬媒体に記録された不正コンテンツも実行、再生出来てしまうことになる。

【０００８】
本発明は、前記従来技術（自明な方式）の課題を解決するもので、可搬媒体に著作権を保持しない不正者によって不正コンテンツが記録されたとしても、実行装置はその可搬媒体に記録されているコンテンツが著作権を保持しない不正者によって記録されたことを検知可能な不正コンテンツ検知システムを提供することを目的とする。
【課題を解決するための手段】
【０００９】
上記課題を解決するために、請求項１における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを受け付ける入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、
を備えることを特徴とする。
【００１０】
請求項２における発明は、コンテンツを実行、もしくは再生する実行装置であって、
前記実行装置は、
認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始する実行部と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記実行部へ渡す取得部と、
を備えることを特徴とする。
【００１１】
請求項３における発明は、請求項２に記載の実行装置であって、
前記取得部は、可搬媒体からデータを取得すること、
を特徴とする。
請求項４における発明は、請求項３に記載の実行装置であって、
前記可搬媒体は光ディスクであり、

前記取得部は、前記光ディスク経由でデータを取得し、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、
を特徴とする。
【００１２】
請求項５における発明は、請求項４に記載の実行装置であって、
前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、
を特徴とする。
請求項６における発明は、請求項２に記載の実行装置であって、
前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、
を特徴とする。
【００１３】
請求項７における発明は、請求項２から請求項６のいずれか１項に記載の実行装置であって、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、
を特徴とする。
【００１４】
請求項８における発明は、請求項２から請求項７のいずれか１項に記載の実行装置であって、
前記実行装置は、さらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、を備え、
前記取得部は、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信し、
前記実行部は、前記暗号化コンテンツを復号化すること、
を特徴とする。
【００１５】
請求項９における発明は、請求項８に記載の実行装置であって、
前記実行装置は、さらに、
デバイス鍵を保持するデバイス鍵格納部と、
前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、
前記取得部はさらに、前記暗号化鍵束を受信すること、
を特徴とする。
【００１６】
請求項１０における発明は、請求項２から請求項９のいずれか１項に記載の実行装置であって、
前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする。
請求項１１における発明は、請求項２から請求項１０のいずれか１項に記載の実行装置であって、
前記検証情報は、デジタル署名方式の検証鍵であること、
を特徴とする。
【００１７】
請求項１２における発明は、請求項２から請求項１１のいずれか１項に記載の実行装置であって、
前記認証情報検証部は、前記検証情報及び前記コンテンツの属性値及び前記配布データ領域特定情報を基に、認証情報を検証すること、

を特徴とする。
【００１８】
請求項１３における発明は、請求項１２に記載の実行装置であって、
前記取得部は、さらに、前記コンテンツの属性値を取得すること、
を特徴とする。
請求項１４における発明は、請求項２から請求項１３のいずれか１項に記載の実行装置であって、
前記コンテンツは、前記実行装置で実行可能なプログラムであり、
前記実行部は、前記プログラムを実行すること、
を特徴とする。
【００１９】
請求項１５における発明は、コンテンツを配布する配布センタであって、
前記配布センタは、
前記コンテンツを受け付ける入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成部と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成部と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布部と、を備え、
を備えることを特徴とする。
【００２０】
請求項１６における発明は、請求項１５に記載の配布センタであって、
前記配布部は、可搬媒体へデータを記録すること、
を特徴とする。
請求項１７における発明は、請求項１６に記載の配布センタであって、
前記可搬媒体は光ディスクであり、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の最終物理アドレスを含むこと、
を特徴とする。
【００２１】
請求項１８における発明は、請求項１７に記載の配布センタであって、
前記配布データ領域特定情報は、さらに、前記コンテンツ及び前記認証情報を前記光ディスクに記録した際の開始物理アドレスを含むこと、
を特徴とする。
請求項１９における発明は、請求項１５に記載の実行装置であって、
前記配布部は、記録媒体、もしくは通信ネットワーク、もしくは放送網を介してデータを配布すること、
を特徴とする。
【００２２】
請求項２０における発明は、請求項１５から請求項１９のいずれか１項に記載の実行装置であって、
前記配布データ領域特定情報は、前記コンテンツ及び前記認証情報を含むデータのデータサイズを含むこと、
を特徴とする。
【００２３】
請求項２１における発明は、請求項１５から請求項２０のいずれか１項に記載の配布センタであって、
前記配布センタはさらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する暗号化部と、を備え、
前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、
を特徴とする。
【００２４】
請求項２２における発明は、請求項２１に記載の配布センタであって、
前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする。
【００２５】
請求項２３における発明は、請求項１５から請求項２２のいずれか１項に記載の配布センタであって、
前記認証情報は、前記検証対象データに対するデジタル署名であること、
を特徴とする。
請求項２４における発明は、請求項１５から請求項２３のいずれか１項に記載の配布センタであって、
前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする。
【００２６】
請求項２５における発明は、請求項１５から請求項２４のいずれか１項に記載の配布センタであって、
前記認証情報生成部は、認証情報生成情報を基に、前記配布データ領域特定情報及び前記コンテンツの属性値を含む検証対象データに対する認証情報を生成すること、
を特徴とする。
【００２７】
請求項２６における発明は、請求項２５に記載の配布センタであって、
前記配布部は、さらに、前記コンテンツの属性値を配布すること、
を特徴とする。
請求項２７における発明は、請求項１５から請求項２６のいずれか１項に記載の配布センタであって、
前記コンテンツはプログラムであること、
を特徴とする。
【００２８】
請求項２８における発明は、不正コンテンツを検知する不正コンテンツ検知方法であって、
前記不正コンテンツ検知方法は、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布手段と、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行手段と、から構成され、
前記配布手段は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、

前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、
前記実行手段は、
前記認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記配布データ領域特定情報を基に、前記認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする。
【００２９】
請求項２９における発明は、コンテンツを実行、もしくは再生する実行方法であって、
前記実行方法は、
認証情報を検証するための検証情報を保持する検証情報格納手段と、
前記検証情報及び前記コンテンツの領域を特定する配布データ領域特定情報を基に、認証情報を検証する認証情報検証手段と、
前記認証情報検証部での検証結果が正当な場合にのみ、取得部経由で取得した前記コンテンツを実行開始、もしくは再生開始するコンテンツ実行手段と、
前記配布データ領域特定情報及び前記認証情報を受け取り、さらに、前記配布データ領域特定情報を基に前記配布データを特定し、前記配布データのみを前記コンテンツ実行手段へ渡す取得手段と、
を備えることを特徴とする。
【００３０】
請求項３０における発明は、コンテンツを配布する配布方法であって、
前記配布方法は、
前記コンテンツを受け付ける入力手段と、
認証情報生成情報を保持する認証情報生成情報格納手段と、
前記実行装置へ配布する前記コンテンツの領域を特定する配布データ領域特定情報を生成する配布データ領域特定情報生成手段と、
前記認証情報生成情報を基に、前記配布データ領域特定情報を含む検証対象データに対する認証情報を生成する認証情報生成手段と、
前記コンテンツと前記配布データ領域特定情報と前記認証情報とを前記実行装置に配布する配布手段と、を備え、
を備えることを特徴とする。

【発明の効果】
【００３１】
不正コンテンツが配布される別の一形態として、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録（追記）されるという場合がありうる。また、別の一形態として、著作権を保持しない不正者によって、正規の著作権者により配布された可搬媒体に記録されている全データを別の可搬媒体にコピーして、その別の可搬媒体で記録可能なデータ領域に不正コンテンツが記録（追記）されるという場合がありうる。このような場合、実行装置においては、正規の著作権者により記録されたデータ（認証情報など）により認証が成功してしまうことで、コンテンツの実行、再生を開始してしまい、最終的には可搬媒体に記録された不正コンテンツも実行、再生出来てしまうことも想定される。上記のような形態を鑑み、本発明の不正コンテンツ検知システムでは、さらに、可搬媒体の中に、可搬媒体に記録されているデータの領域を識別する配布データ領域特

定情報（例えば、データが記録されている開始物理アドレスと最終物理アドレス、もしくは、記録データサイズなど）と、その配布データ領域特定情報に対する著作権者の認証情報（例えば、デジタル署名。属性値に対するデジタル署名と兼ねてもよい）とを記録しておく。そして、実行装置の取得部では、可搬媒体に記録された配布データ領域特定情報を受け取った場合、その配布データ領域特定情報で指定された領域外のデータは取得部の外部からの要求でも取得しないようにする。このようにすることによって、正規の著作権者により配布された可搬媒体に記録可能なデータ領域が残っている場合に、著作権を保持しない不正者によってその記録可能なデータ領域に不正コンテンツが記録されたとしても、取得部は予め著作権者によって指定された領域外のデータは取得しないため、不正コンテンツを実行、再生出来ないようになる。また、実行装置では、さらに、可搬媒体に記録された配布データ領域特定情報が著作権者によって記録されたものかどうか、認証情報を基に検証し、検証が失敗した場合、該当する可搬媒体に記録されているコンテンツは実行開始、再生開始しないようにした。そうすることによって、著作権が保持しない不正者が、可搬媒体の記録されている配布データ領域特定情報を改ざんしたとしても、その可搬媒体に記録されているコンテンツは実行、再生しないようになった。このことにより、著作権を保持しない不正者によって不正コンテンツが記録（追記）されるという不正行為を防ぐことが出来るようになった。

【００３２】

また、実行装置において、配布された不正コンテンツが実行、再生される不正行為の別の一形態として、可搬媒体に記録されているデータを読み出すドライブ部と、ドライブ部によって取得されたデータを実行、再生するコンテンツ実行部との間に流れるデータを改竄される場合がある。例えば、著作権を保持しない不正者は、正規の著作権者による配布データ領域特定情報と対応する認証情報を取得しているものとする。その場合、その不正者は、不正な可搬媒体に、任意の配布データ領域特定情報と、偽の認証情報とを記録する。それにより、実行装置のドライブ部においては、その不正な可搬媒体に記録されている配布データ領域特定情報を基にして、その配布データ領域特定情報で指定された領域のデータはコンテンツ実行部からの要求で取得出来るようになる。続いて、実行装置のドライブ部が、その不正な可搬媒体に記録されている配布データ領域特定情報と、その配布データ領域特定情報に対する認証情報をコンテンツ実行部へ出力しようとする。その際、不正者は、ドライブ部が出力した配布データ領域特定情報と認証情報を、正規の著作権者による配布データ領域特定情報と対応する認証情報に差し替えて、コンテンツ実行部へ出力する。それにより、コンテンツ実行部では、正規の著作権者による配布データ領域特定情報と対応する認証情報を基に暗号化コンテンツの検証を行うため、検証が成功する。よって、コンテンツ実行部はコンテンツの実行、再生を開始してしまう。上記のような不正行為を鑑み、本発明の不正コンテンツ検知システムでは、ドライブ部からコンテンツ実行部へ出力するデータの一部（例えば、配布データ領域特定情報）を暗号化して出力するようにした。これにより、不正者は、ドライブ部が出力したデータを別のデータに差し替えてコンテンツ実行部へ出力しようとしても、不正者は正しく暗号化することが出来ないため、正しくコンテンツ実行部へ出力できなくなった。この際、同じデータであっても、ドライブ部からコンテンツ実行部へ出力する暗号文が異なるようにしてもよい。これは、例えば、ドライブ部とコンテンツ実行部が毎回異なるセッション鍵を共有することにより実現出来る。このことにより、著作権を保持しない不正者によって不正コンテンツが実行、再生されるという不正行為を防ぐことが出来るようになった。

【発明を実施するための最良の形態】

【００３３】

以下本発明の実施の形態について、図面を参照しながら説明する。

（実施の形態１）

著作権を保持しない不正者により、不正コンテンツが記録された可搬媒体が配布された場合に、実行装置では不正者により配布された可搬媒体に記録されている不正コンテンツ

が実行、再生出来ないようにすることが望まれる。このように、不正者により不正コンテンツが記録された可搬媒体が配布される不正行為には、例えば、以下で示すような不正行為が挙げられる。その不正行為は、不正者が、正規の配布センタによって配布された可搬媒体に記録されているコンテンツの全部を新たな可搬媒体へ記録して、さらに、その新たな可搬媒体の記録されていない部分に不正コンテンツを記録する不正行為である。その不正行為においては、新たな可搬媒体には、正規の配布センタによって配布されたデータがそのまま記録されているため、新たな可搬媒体には著作権者によって記録されたコンテンツが格納されていると判断してしまう場合がある。これを利用して、不正者は実行装置で不正コンテンツを実行、再生させることを試みるという不正行為である。本発明の実施の形態１では、上記の不正行為を想定し、そのような不正コンテンツが記録された可搬媒体が配布された場合にでも、実行装置では不正者により配布された可搬媒体に記録されている不正コンテンツが実行、再生出来ないようにすることを目的とする。

【００３４】

本発明の実施の形態１では、上記不正行為に対する対策として、配布センタは、著作権者によって可搬媒体に記録されたデータのデータ領域の領域である配布データ領域特定情報を記録するようにして、実行装置では、その配布データ領域特定情報で指定されたデータ領域の領域外にあるデータは取得しないようにした。このことにより、実行装置では配布データ領域特定情報により予め著作権者によって指定された領域外のデータは取得しないため、可搬媒体に格納されている不正コンテンツを実行、再生出来ないようになる。また可搬媒体には、さらに、配布データ領域特定情報に対する認証情報を記録するようにして、実行装置では、認証情報が可搬媒体に記録された配布データ領域特定情報に対する正規の著作権者の認証情報であるか検証し、検証が成功した場合にのみ、コンテンツの実行、再生を行うようにした。このことにより、著作権を保持しない不正者が、可搬媒体の記録されている配布データ領域特定情報を改ざんしたとしても、その可搬媒体に記録されているコンテンツは実行、再生しないようになった。このことにより、上記不正行為に対する耐性を向上させる。

【００３５】

図１は、本発明の実施の形態１における不正コンテンツ検知システムの構成図である。図１において、配布センタ１０は外部からコンテンツＣＮＴを受け取り、後述する実行装置１２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体１１に記録するものであり、可搬媒体１１は実行装置１２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置１２は可搬媒体１１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。

【００３６】

不正コンテンツ検知システム１は、配布センタ１０（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等の可搬媒体１１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、暗号化コンテンツＥＮＣＣＮＴを基に生成される第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇと第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと、可搬媒体１１に記録されたデータのデータ領域の領域である配布データ領域特定情報ＡＲＥＡと、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡの正当性を示す情報である認証情報ＡＵＴＨを、各実行装置１２へ配布する。各実行装置１２は、暗号化コンテンツＥＮＣＣＮＴを基に第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇと第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部の情報を入れ替えて入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を作成し、認証情報ＡＵＴＨが配布センタ１０による入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡの正規の認証情報であることを確認し、コンテンツＣＮＴを実行開始する。

【００３７】

以上が、本実施の形態の概要である。以下に、本発明の不正コンテンツ検知システムの

一実施の形態である不正コンテンツ検知システム１の詳細について説明を行う。
＜不正コンテンツ検知システム１の構成＞
不正コンテンツ検知システム１は、図１に示すように、配布センタ１０と、可搬媒体１１と、ｓ個の実行装置１２（ｓは１以上の自然数）から構成される。
【００３８】
以下に、これらの構成要素について、詳細に説明する。まず、配布センタ１０の構成と動作について述べ、続いて可搬媒体１１の構成について述べ、最後に実行装置１２の構成と動作について述べる。
＜配布センタ１０の構成＞
配布センタ１０は、図２に示すように、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、暗号化部１００５、ハッシュテーブル生成部１００６、可搬媒体イメージ生成部１００７、配布データ領域特定情報生成部１００８、認証情報生成情報格納部１００９、認証情報生成部１０１０、記録部１０１１から構成される。
【００３９】
（１）入力部１００１
入力部１００１は、外部からコンテンツＣＮＴを入力出来るものである。入力部１００１は、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭやビデオテープ、映画フィルム等からコンテンツＣＮＴを読み取る機能を有する。コンテンツＣＮＴは、例えば、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）２フォーマット形式による動画データやＭＰ３フォーマットによる音声データである。外部からコンテンツＣＮＴが入力された場合、コンテンツ鍵生成要求ＲＥＱをコンテンツ鍵生成部１００２へ出力し、コンテンツＣＮＴを暗号化部１００５へ出力する。なお、外部から入力されるコンテンツＣＮＴは、実行装置１２で実行可能なフォーマット形式であるとしたが、これに限るものではない。例えば、実行装置１２で実行可能なフォーマット形式ではない場合、入力部１００１は、実行装置１２で実行可能なフォーマット形式への変換処理を実施するようにしてもよい。
【００４０】
（２）コンテンツ鍵生成部１００２
コンテンツ鍵生成部１００２は、入力部１００１からコンテンツ鍵生成要求ＲＥＱが入力された場合、コンテンツ鍵ＣＫを生成する。コンテンツ鍵ＣＫを生成する方法としては、例えば、乱数を用いて１２８ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部１００２が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵ＣＫを暗号化鍵束生成部１００４及び暗号化部１００５へ出力する。なお、コンテンツ鍵ＣＫはコンテンツＣＮＴを暗号化、復号化するための鍵であり、暗号化部１００５及び実行装置１２の実行部１２１７で使用される。
【００４１】
（３）実行装置情報格納部１００３
実行装置情報格納部１００３は、複数の実行装置１２に与えられる鍵情報を保持するものである。図３は、実行装置情報格納部１００３の一例を示しており、装置識別子ＡＩＤ１に対応付けられたデバイス鍵ＤＫ１と、装置識別子ＡＩＤ２に対応付けられたデバイス鍵ＤＫ２と、・・・、装置識別子ＡＩＤｓに対応付けられたデバイス鍵ＤＫｓを保持している状態を示している。ここで、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｓのそれぞれは、複数の実行装置１２のいずれかに対応付けられており、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｓのそれぞれは、対応する実行装置１２のデバイス鍵格納部１２１１に格納されている鍵である。なお、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｓのそれぞれはコンテンツ鍵ＣＫを暗号化、復号化するための鍵であり、暗号化鍵束生成部１００４及びコンテンツ鍵取得部１２１２で用いられる。例えば、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｓは、それぞれ異なる自然数１、２、・・・、ｎであり、デバイス鍵Ｄ

Ｋ１、ＤＫ２、・・・、ＤＫｓは、例えば、それぞれ異なる１２８ビット鍵データである。

【００４２】

（４）暗号化鍵束生成部１００４

暗号化鍵束生成部１００４は、コンテンツ鍵生成部１００２からコンテンツ鍵ＣＫが入力された場合、実行装置情報格納部１００３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢは、各実行装置１２がその暗号化鍵束ＫＢと自身の保持する鍵を用いてコンテンツ鍵ＣＫが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置１２はそれぞれ、ＡＩＤ１からＡＩＤｓのいずれかの装置識別子と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｓのいずれか）を保持しており、実行装置情報格納部１００３には、図３のように、実行装置１２が保持する装置識別子（ＡＩＤ１、・・・、ＡＩＤｓ）と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｓ）の組が全て格納されているとする。そのような場合、暗号化鍵束ＫＢは例えば以下のように生成される。実行装置情報格納部１００３から装置識別子ＡＩＤ１と対応するデバイス鍵ＤＫ１を取得する。そして、デバイス鍵ＤＫ１を基にコンテンツ鍵ＣＫを暗号化し、暗号化コンテンツ鍵ＥＮＣＣＫ１＝Ｅｎｃ（ＤＫ１、ＣＫ）を生成し、装置識別子ＡＩＤ１に対応付ける。なお、Ｅｎｃ（Ｋ、Ｐ）を平文Ｐを暗号化鍵Ｋで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子（ＡＩＤ２、・・・、ＡＩＤｓ）とデバイス鍵（ＤＫ２、・・・、ＤＫｓ）に対しても同様の処理を行い、暗号化コンテンツ鍵ＥＮＣＣＫ２＝Ｅｎｃ（ＤＫ２、ＣＫ）、・・・、ＥＮＣＣＫｎ＝Ｅｎｃ（ＤＫｓ、ＣＫ）を生成し、装置識別子ＡＩＤ２、・・・、ＡＩＤｓに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のｓ組から構成される、図４のような暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢをこのような構成にすることによって、各実行装置１２はその暗号化鍵束ＫＢと自身の保持するデバイス鍵（ＤＫ１、・・、ＤＫｓの何れか）を用いてコンテンツ鍵ＣＫが取得出来るようになる。そして、暗号化鍵束ＫＢを可搬媒体イメージ生成部１０１１に出力する。なお、特許文献２などに記載の方法を用いることで、暗号化鍵束ＫＢの中の暗号化コンテンツ鍵（先程の例ではｓ個）の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵ＣＫを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部１００４で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置１２のコンテンツ鍵取得部１２１２と同じ暗号アルゴリズムを用いる。

【００４３】

（５）暗号化部１００５

暗号化部１００５は、入力部１００１からコンテンツＣＮＴを入力され、さらに、コンテンツ鍵生成部１００２からコンテンツ鍵ＣＫとが入力された場合、以下のようにして暗号化コンテンツＥＮＣＣＮＴを生成する。ここで、コンテンツＣＮＴは、図５で示すように、ｎ個（ｎは２以上の自然数）の部分コンテンツＣＮＴ＃１、ＣＮＴ＃２、ＣＮＴ＃３、・・・、ＣＮＴ＃ｎから構成されるとする。コンテンツＣＮＴがｎ個の部分コンテンツから構成されている一例としては、コンテンツＣＮＴが複数のファイルから構成されている場合が挙げられる。例えば、コンテンツＣＮＴがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合の、ＶＯＢ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ）ファイル等で分割されている。また、コンテンツＣＮＴが複数のＭＰＥＧ２形式の動画コンテンツから構成されている場合や、複数のＭＰ３形式の音声コンテンツから構成されている場合もある。なお、ＤＶＤ－Ｖｉｄｅｏ形式については、 HYPERLINK "例えばインターネットアドレスhttp://positron.jfet.org/dvdvideo.html" 例えばインターネットアドレスhttp://positron.jfet.org/dvdvideo.htmlに記載されており、ＭＰＥＧ形式については、例えばインターネットアドレス HYPERLINK "http://www.pioneer.co.jp/crdl/tech/mpeg/1.html" http://www.pioneer.co.jp/crdl/tech/mpeg/1.htmlに記載されている。

【００４４】

そして、コンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ＃１を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ＃１＝Ｅｎｃ（ＣＫ、ＣＮＴ＃１）を生成する。続いて、同じコンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ＃２を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ＃２＝Ｅｎｃ（ＣＫ、ＣＮＴ＃２）を生成する。これを繰り返して、図５で示すようなｎ個の暗号化部分コンテンツＥＮＣＣＮＴ＃１、・・・、ＥＮＣＣＮＴ＃ｎから構成される暗号化コンテンツＥＮＣＣＮＴを生成する。暗号化部１００５で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置１２の実行部１２１７と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツＥＮＣＣＮＴの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵ＣＫで暗号化していたが、非特許文献１に記載のブロック暗号のモードを利用してもよい。例えば、ＣＢＣモードやＯＦＢモード、ＣＦＢモードなどでもよく、さらに、ある一定間隔毎にモード（例：ＣＢＣモード）の初期値を変化させるようにしたものでも良い。

【００４５】

続いて、ｎ個の暗号化部分コンテンツのそれぞれを識別、特定出来る、ｎ個の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎを取得する。このｎ個の特定情報は、例えば、暗号化コンテンツＥＮＣＣＮＴが複数のファイルから構成されている場合、各ファイルのファイル名である。ここでは、暗号化部分コンテンツＥＮＣＣＮＴ＃１を識別、特定する情報を特定情報ＡＤＤＲ＃１、暗号化部分コンテンツＥＮＣＣＮＴ＃２を識別、特定する情報を特定情報ＡＤＤＲ＃２、暗号化部分コンテンツＥＮＣＣＮＴ＃３を識別、特定する情報を特定情報ＡＤＤＲ＃３、・・・、暗号化部分コンテンツＥＮＣＣＮＴ＃ｎを識別、特定する情報を特定情報ＡＤＤＲ＃ｎとする。そして、暗号化コンテンツＥＮＣＣＮＴを可搬媒体イメージ生成部１００７へ出力し、暗号化部分コンテンツと特定情報のｎ組｛ＥＮＣＣＮＴ＃１、ＡＤＤＲ＃１｝、｛ＥＮＣＣＮＴ＃２、ＡＤＤＲ＃２｝、・・・、｛ＥＮＣＣＮＴ＃ｎ、ＡＤＤＲ＃ｎ｝を、ハッシュテーブル生成部１００６へ出力する。

【００４６】

なお、それぞれの特定情報は、上記で紹介した情報に限らず、各暗号化部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。例えば、暗号化部分コンテンツの先頭の論理アドレスとサイズ（オフセット）、もしくは、先頭と終端の論理アドレス、もしくは、先頭の物理アドレスとサイズ（オフセット）、もしくは、先頭と終端の物理アドレス、などでもよい。

【００４７】

（６）ハッシュテーブル生成部１００６

ハッシュテーブル生成部１００６は、暗号化部１００５から、暗号化部分コンテンツと特定情報のｎ組｛ＥＮＣＣＮＴ＃１、ＡＤＤＲ＃１｝、｛ＥＮＣＣＮＴ＃２、ＡＤＤＲ＃２｝、・・・、｛ＥＮＣＣＮＴ＃ｎ、ＡＤＤＲ＃ｎ｝とが入力された場合、以下のようにして、第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを生成する。

【００４８】

ｎ組の暗号化部分コンテンツと特定情報から第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを生成する大まかな流れは、図６で示す通りである。まず、ｎ組の暗号化部分コンテンツと特定情報のそれぞれの組に対して、第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、ＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎを生成する。そして、ｎ個の第一ハッシュテーブルから構成される第一ハッシュテーブル群及び特定情報を用いて第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを生成する。

【００４９】

まず、ｎ組の暗号化部分コンテンツと特定情報のそれぞれの組に対して、第一ハッシュテーブルを生成する方法について説明する。ここでは例として、暗号化部分コンテンツＥＮＣＣＮＴ＃１と特定情報ＡＤＤＲ＃１から第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１

を生成する方法について説明する。なお、暗号化部分コンテンツＥＮＣＣＮＴ＃２と特定情報ＡＤＤＲ＃２、・・・、ＥＮＣＣＮＴ＃ｎと特定情報ＡＤＤＲ＃ｎから第一ハッシュテーブルＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎのそれぞれを生成する方法は、暗号化部分コンテンツＥＮＣＣＮＴ＃１と特定情報ＡＤＤＲ＃１から第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１を生成する方法と同じであるため、説明を省略する。まず、図７で示すように、暗号化部分コンテンツＥＮＣＣＮＴ＃１をｍ個（ｍは１以上の自然数）のユニットＵ＃１、Ｕ＃２、・・・、Ｕ＃ｍに分割する。分割する方法の一例としては、例えば暗号化部分コンテンツをある所定のサイズ毎に分割する方法がある。例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位などである。ここで、暗号化部分コンテンツを所定のサイズ毎に分割した場合に余りのデータが出てしまう場合、余りとなった部分は一つのユニットとして扱わないようにする。なお、余りとなった部分に足りない部分をある所定の値（たとえば０など）で補充して、一つのユニットとして扱うようにしても良い。そして、ｍ個のユニットのそれぞれを識別可能な第一識別子を生成する。第一識別子を生成する方法としては、例えば、各ユニットに自然数を順番に割り当てていく（１、２、・・・、ｍ）方法などがある。ここで、各組に対して生成した第一識別子をそれぞれ、ＩＤ１＃１、ＩＤ１＃２、・・・ＩＤ１＃ｍとし、次のように第一識別子とユニットが対応しているとする。｛ＩＤ１＃１、Ｕ＃１｝、｛ＩＤ１＃２、Ｕ＃２｝、・・・、｛ＩＤ１＃ｍ、Ｕ＃ｎ｝。続いて、ｍ組の第一識別子とユニットの各組に対して、ユニットの属性値（ハッシュ値）として第一ハッシュ値を計算する。ユニットの属性値である第一ハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置１２の認証情報検証部１２１６で用いる方法と同じものを用いる。ここで、各組に対して計算した属性値だる第一ハッシュ値をそれぞれ、ＨＡＳＨ１＃１、ＨＡＳＨ１＃２、・・・、ＨＡＳＨ１＃ｍとし、次のように第一識別子とユニットと第一ハッシュ値とが対応しているとする。｛ＩＤ１＃１、Ｕ＃１、ＨＡＳＨ１＃１｝、｛ＩＤ１＃２、Ｕ＃２、ＨＡＳＨ１＃２｝、・・・、｛ＩＤ１＃ｍ、Ｕ＃ｍ、ＨＡＳＨ１＃ｍ｝。最後に、その中から第一識別子と第一ハッシュ値を抜き出し、第一ハッシュテーブルＨＡＳＨＴＢＬ＃１＝｛ＩＤ１＃１、ＨＡＳＨ１＃１｝、｛ＩＤ１＃２、ＨＡＳＨ１＃２｝、・・・、｛ＩＤ１＃ｍ、ＨＡＳＨ１＃ｍ｝を生成する。なお、暗号化部分コンテンツをｍ個のユニットに分割する方法は、上記の方法に限るものではない。例えば、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、セル（Ｃｅｌｌ）単位などでもよい。また、コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などでもよい。コンテンツデータがディスクに記録されている場合、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（ＥＣＣブロック単位）などでもよい。なお、第一識別子は、上記の方法によって生成されたものに限るものではない。例えば、各ユニットを識別可能な論理アドレスや物理アドレスでもよいし、乱数を用いてランダムな自然数を割り当ててもよい。

【００５０】

続いて、ｎ個の第一ハッシュテーブルと対応するｎ個の特定情報を用いて第二ハッシュテーブルＨＡＳＨＴＢＬ２を生成する方法について、図８を用いて説明する。まず、ｎ組の特定情報と第一ハッシュテーブルのそれぞれに対して、第一ハッシュテーブルの属性値（ハッシュ値）として第二ハッシュ値を計算する。第一ハッシュテーブルの第二ハッシュ値を求める方法としては、例えばｍ個の第一ハッシュ値と第一識別子の値を連結した値を一方向性関数に入力した場合の出力値を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置１２の認証情報検証部１２１６で用いる方法と同じものを用いる。ここで、各組に対して計算した第二ハッシュ値をそれぞれ、ＨＡＳＨ２＃１、ＨＡＳＨ２＃２、・・・、ＨＡＳＨ２＃ｎとし、次のように特定情報と第一ハッシュテーブルと第二ハッシュ値が対応しているとする。｛ＡＤＤＲ＃１、ＨＡＳＨＴＢＬ１＃１、ＨＡＳＨ２＃１｝、｛ＡＤＤＲ＃２、ＨＡ

ＳＨＴＢＬ１＃２、ＨＡＳＨ２＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＨＡＳＨＴＢＬ１＃ｎ、ＨＡＳＨ２＃ｎ｝。その中から特定情報と第二ハッシュ値とを抜き出し、第二ハッシュテーブルＨＡＳＨＴＢＬ２＝｛ＡＤＤＲ＃１、ＨＡＳＨ２＃１｝、｛ＡＤＤＲ＃２、ＨＡＳＨ２＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＨＡＳＨ２＃ｎ｝を生成する。

【００５１】

そして、ｎ個の特定情報を用いてコンテンツ位置情報ＰＯＳを生成する方法について説明する。まず、それぞれの特定情報ＡＤＤＲ＃１、ＡＤＤＲ＃２、・・・、ＡＤＤＲ＃ｎに対して、対応する暗号化部分コンテンツを分割した際のユニットの個数であるユニット数をそれぞれＮＵＭＵ＃１、ＮＵＭＵ＃２、・・・、ＮＵＭＵ＃ｎとする。そして、図９で示すような、そのｎ組の特定情報とユニット数から構成される、コンテンツ位置情報ＰＯＳ＝｛ＡＤＤＲ＃１、ＮＵＭＵ＃１｝、｛ＡＤＤＲ＃２、ＮＵＭＵ＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＮＵＭＵ＃ｎ｝を生成する。

【００５２】

最後に、ｎ個の第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、ＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎから構成される第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを、可搬媒体イメージ生成部１００７へ出力する。そして、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを、認証情報生成部１０１０へ出力する。

【００５３】

（７）可搬媒体イメージ生成部１００７

可搬媒体イメージ生成部１００７は、暗号化鍵束生成部１００４から暗号化鍵束ＫＢとが入力され、ハッシュテーブル生成部１００６から第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳとが入力され、暗号化部１００５から暗号化コンテンツＥＮＣＣＮＴとが入力された場合、図１０で示すような、可搬媒体１１に記録するデータのイメージである可搬媒体イメージＩＭＧを生成する。この可搬媒体イメージＩＭＧは、例えば、可搬媒体１１に記録した場合の物理アドレスを取得出来るものである。ここで、可搬媒体イメージＩＭＧには、認証情報生成部１０１０で生成される認証情報ＡＵＴＨを挿入するためにスペースを空けておくようにする。そして、その可搬媒体イメージＩＭＧを配布データ領域特定情報生成部１００８及び記録部１０１１へ出力する。

【００５４】

（８）配布データ領域特定情報生成部１００８

配布データ領域特定情報生成部１００８、可搬媒体イメージ生成部１００７から可搬媒体イメージＩＭＧとが入力された場合、可搬媒体１１に記録するデータの領域を識別する配布データ領域特定情報ＡＲＥＡを取得、もしくは生成する。この配布データ領域特定情報ＡＲＥＡは、例えば、可搬媒体１１に記録するデータの開始物理アドレスと最終物理アドレスの組である。もしくは、配布データ領域特定情報ＡＲＥＡは、例えば、可搬媒体１１に記録するデータの最初物理アドレスと最終物理アドレスの組である。もしくは、配布データ領域特定情報ＡＲＥＡは、例えば、可搬媒体１１に記録するデータの最初物理アドレスと最終物理アドレスの複数の組である。そして、その配布データ領域特定情報ＡＲＥＡを認証情報生成部１０１０及び記録部１０１１へ出力する。

【００５５】

（９）認証情報生成情報格納部１００９

認証情報生成情報格納部１００９は、第二ハッシュテーブル群ＨＡＳＨＴＢＬ２Ｇとコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡの正当性を示す認証情報である認証情報ＡＵＴＨを生成するための、認証情報生成情報ＧＥＮＡＵＴＨが予め与えられ、保持するものである。この認証情報生成情報ＧＥＮＡＵＴＨは、例えば、デジタル署名アルゴリズムの署名生成鍵（秘密鍵）である。認証情報生成情報ＧＥＮＡＵＴＨに対応する検証情報ＶＥＲは、実行装置１２の検証情報格納部１２１５に格納されている。この検証情報ＶＥＲは、例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デ

ジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式やＲＳＡ署名などである。

【００５６】

（１０）認証情報生成部１０１０

認証情報生成部１０１０は、ハッシュテーブル生成部１００６から第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳとが入力され、配布データ領域特定情報生成部１００８から配布データ領域特定情報ＡＲＥＡとが入力された場合、以下のようにして、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡを含む検証対象データに対する認証情報ＡＵＴＨを生成する。まず、認証情報生成情報格納部１００９にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、図１１で示すように、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳ及び配布データ領域特定情報ＡＲＥＡと認証情報生成情報ＧＥＮＡＵＴＨを用いて、認証情報ＡＵＴＨを生成する。なお、認証情報ＡＵＴＨの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズムを用いる方法の一例を説明する。まず、第二ハッシュテーブルＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とｎ個の特定情報と、コンテンツ位置情報ＰＯＳに含まれるｎ個の特定情報とｎ個のユニット数から、第二ハッシュ値と特定情報とユニット数のｎ組を生成する。そして、それらの値と配布データ領域特定情報ＡＲＥＡの値を連結した値に対するデジタル署名を作成する。ここで、ＧＥＮＳＩＧ（Ｋ、Ｍ）は署名生成鍵Ｋを用いてメッセージＭに対して生成されたデジタル署名とすると、認証情報ＡＵＴＨは、ＡＵＴＨ＝ＧＥＮＳＩＧ（ＧＥＮＡＵＴＨ、｛ＨＡＳＨ２＃１｜｜ＡＤＤＲ＃１｜｜ＮＵＭＵ＃１｝｜｜｛ＨＡＳＨ２＃２｜｜ＡＤＤＲ＃２｜｜ＮＵＭＵ＃１｝｜｜・・・｜｜｛ＨＡＳＨ２＃ｎ｜｜ＡＤＤＲ＃ｎ｜｜ＮＵＭＵ＃ｎ｝｜｜ＡＲＥＡ）となる。そして、認証情報ＡＵＴＨを記録部１０１１へ出力する。なお、認証情報生成部１０１０で使用するデジタル署名アルゴリズムは、実行装置１２の認証情報検証部１２１６で用いるデジタル署名アルゴリズムと同じものを用いる。

【００５７】

（１１）記録部１０１１

記録部１０１１は、配布データ領域特定情報生成部１００８から可搬媒体イメージＩＭＧが入力され、認証情報生成部１０１０から認証情報ＡＵＴＨが入力された場合、可搬媒体イメージＩＭＧに予め確保されているデータ領域に認証情報ＡＵＴＨを挿入して、図１２で示すような第二可搬媒体イメージＩＭＧ２を生成する。そして、第二可搬媒体イメージＩＭＧ２を可搬媒体１１へ記録する。例えば、可搬媒体１１は光ディスク（ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ）であり、記録部１０１１は与えられた第二可搬媒体イメージを基に光ディスクをプレス製造する機能を有する。なお、可搬媒体１１は書き込み可能光ディスク（ＣＤ－ＲやＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭなど）であり、記録部１０１１は書き込み用レーザー等を用いて、与えられた第二可搬媒体イメージを基に光ディスクにデータを書き込む機能を有していてもよい。

【００５８】

＜配布センタ１０の動作＞

以上で、配布センタ１０の構成について説明を行ったが、ここでは配布センタ１０の動作の一例について、図１３に示すフローチャートの処理を行う。なお、配布センタ１０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【００５９】

入力部１００１は、外部から入力されたコンテンツＣＮＴを暗号化部１００５へ出力し、コンテンツ鍵生成要求ＲＥＱをコンテンツ鍵生成部１００２へ出力する（ステップＳ１０１）。

コンテンツ鍵生成要求ＲＥＱを入力されたコンテンツ鍵生成部１００２は、コンテンツ鍵ＣＫを生成し、コンテンツ鍵ＣＫを暗号化鍵束生成部１００４及び暗号化部１００５へ

出力する（ステップＳ１０２）。
【００６０】
コンテンツ鍵ＣＫを入力された暗号化鍵束生成部１００４は、実行装置情報格納部１００３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。そして、暗号化鍵束ＫＢを記録部１０１１に出力する（ステップ１０３）。
コンテンツＣＮＴ及びコンテンツ鍵ＣＫが入力された暗号化部１００５は、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化コンテンツＥＮＣＣＮＴを可搬媒体イメージ生成部１００７へ出力し、ｎ組の暗号化部分コンテンツと特定情報を、ハッシュテーブル生成部１００６へ出力する（ステップＳ１０４）。
【００６１】
ｎ組の暗号化部分コンテンツと特定情報を入力されたハッシュテーブル生成部１００６は、ｎ個の第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、・・・、ＨＡＳＨＴＢＬ１＃ｎから構成される第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを生成する。そして、第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置特定情報ＰＯＳを可搬媒体イメージ生成部１００７へ出力し、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置特定情報ＰＯＳを認証情報生成部１０１０へ出力する（ステップＳ１０５）。
【００６２】
可搬媒体イメージ生成部１００７は、暗号化鍵束生成部１００４から暗号化鍵束ＫＢとが入力され、ハッシュテーブル生成部１００６から第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳとが入力され、暗号化部１００５から暗号化コンテンツＥＮＣＣＮＴとが入力された場合、可搬媒体１１に記録するデータのイメージである可搬媒体イメージＩＭＧを生成する。そして、その可搬媒体イメージＩＭＧを配布データ領域特定情報生成部１００８及び記録部１０１１へ出力する。（ステップＳ１０６）
配布データ領域特定情報生成部１００８は、可搬媒体イメージ生成部１００７から可搬媒体イメージＩＭＧとが入力された場合、可搬媒体１１に記録するデータの領域を識別する配布データ領域特定情報ＡＲＥＡを取得、もしくは生成する。そして、その配布データ領域特定情報ＡＲＥＡを認証情報生成部１０１０及び記録部１０１１へ出力する。（ステップＳ１０７）
第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡを入力された認証情報生成部１０１０は、認証情報生成情報格納部１００９にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、認証情報生成情報ＧＥＮＡＵＴＨを用いて、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡの正当性を示す認証情報である認証情報ＡＵＴＨを生成する。そして、認証情報ＡＵＴＨを記録部１０１１へ出力する（ステップＳ１０８）。
【００６３】
記録部１０１１は、可搬媒体イメージ生成部１００７から可搬媒体イメージＩＭＧが入力され、認証情報生成部１０１０から認証情報ＡＵＴＨが入力された場合、可搬媒体イメージＩＭＧに認証情報ＡＵＴＨを挿入して第二可搬媒体イメージＩＭＧ２を生成し、その第二搬媒体イメージＩＭＧ２を可搬媒体１１へ記録する。（ステップＳ１０９）
以上が、不正コンテンツ検知システム１の構成要素である配布センタ１０の構成と動作である。続いて、可搬媒体１１の構成について説明を行う。
【００６４】
＜可搬媒体１１の構成＞
可搬媒体１１は、例えば、ＤＶＤ－ＲＯＭやＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＣＤ－ＲＯ

Ｍ、ＣＤ－Ｒ等のような光ディスクの媒体（メディア）であり、図１４に示すように、暗号化鍵束ＫＢと第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇと第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが配布センタ１０によって記録されているものとする。

【００６５】

以上が、不正コンテンツ検知システム１の構成要素である可搬媒体１１の構成である。続いて、実行装置１２の構成と動作について説明を行う。

＜実行装置１２の構成＞

実行装置１２は、図１５に示すように、大きくドライブ部１２０とコンテンツ実行部１２１から構成される。ドライブ部１２０とコンテンツ実行部１２１は、例えば、バスなどにより接続されている。ドライブ部１２０は、読取部１２０１、配布データ領域特定情報格納部１２０２、第一秘密鍵格納部１２０３、第一秘匿通信処理部１２０４とから構成される。コンテンツ実行部１２１は、デバイス鍵格納部１２１１、コンテンツ鍵取得部１２１２、第二秘密鍵格納部１２１３、第二秘匿通信処理部１２１４、検証情報格納部１２１５、認証情報検証部１２１６、実行部１２１７とから構成される。

【００６６】

（１）読取部１２０１

読取部１２０１は、可搬媒体１１に記録されているデータの読み取りを行う。読取部１２０１は、実行装置１２が可搬媒体１１のデータを読み取り可能になった場合に、まず、可搬媒体１１に記録されている配布データ領域特定情報ＡＲＥＡを取得し、配布データ領域特定情報格納部１２０２に格納する。そして、その配布データ領域特定情報ＡＲＥＡを第一秘匿通信処理部１２０４へ出力する。その後、可搬媒体１１に記録されている暗号化鍵束ＫＢ及びコンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨを取得し、暗号化鍵束ＫＢをコンテンツ鍵取得部１２１２へ出力し、コンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨを認証情報検証部１２１６へ出力する。

【００６７】

また、読取部１２０１は、認証情報検証部１２１６もしくは実行部１２１７から可搬媒体１１に記録されているデータの読取要求が来た場合、まず配布データ領域特定情報格納部１２０２に格納されている配布データ領域特定情報ＡＲＥＡを取得する。そして、認証情報検証部１２１６もしくは実行部１２１７から読取要求が来たデータが配布データ領域特定情報ＡＲＥＡで識別される記録領域内であれば、可搬媒体１１に記録されているデータ（第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２及び暗号化コンテンツＥＮＣＣＮＴの全部、もしくは、一部）を取得して、読取要求が来た認証情報検証部１２１６もしくは実行部１２１７に出力する。例えば、配布データ領域特定情報ＡＲＥＡが可搬媒体１１に記録されているデータの開始物理アドレスと最終物理アドレスを示している場合、読取要求が来たデータが配布データ領域特定情報ＡＲＥＡである開始物理アドレスよりも後の（大きい）アドレスにあり、かつ、最終物理アドレスよりも前の（小さい）アドレスにある場合、その該当データを認証情報検証部１２１６もしくは実行部１２１７に出力する。認証情報検証部１２１６もしくは実行部１２１７から読取要求が来たデータが配布データ領域特定情報ＡＲＥＡで識別される記録領域外であれば、読取要求が来た認証情報検証部１２１６もしくは実行部１２１７へはデータは出力しない。例えば、配布データ領域特定情報ＡＲＥＡが可搬媒体１１に記録されているデータの開始物理アドレスと最終物理アドレスを示している場合、読取要求が来たデータが配布データ領域特定情報ＡＲＥＡである開始物理アドレスよりも前の（小さい）アドレスであるか、もしくは、最終物理アドレスよりも後の（大きい）アドレスにある場合、その該当データを認証情報検証部１２１６もしくは実行部１２１７へ出力しない。

【００６８】

（２）配布データ領域特定情報格納部１２０２

配布データ領域特定情報格納部１２０２は、可搬媒体１１に記録されている配布データ

領域特定情報ＡＲＥＡを保持するものである。配布データ領域特定情報ＡＲＥＡは、例えば、可搬媒体１１に記録されているデータの開始物理アドレスと最終物理アドレスの組である。

【００６９】

（３）第一秘密鍵格納部１２０３

第一秘密鍵格納部１２０３は、第一秘匿通信処理部１２０４と第二秘匿通信処理部１２１４との間で秘匿通信を行うための鍵情報を保持するものであり、予め与えられる１２８ビットの鍵情報である共通秘密鍵ＳＫを保持する。与えられる共通秘密鍵ＳＫの値は、第二秘密鍵格納部１２１３が保持する共通秘密鍵ＳＫの値と同じである。なお、第一秘密鍵格納部１２０３は、共通秘密鍵ＳＫではなく、公開鍵暗号用の鍵情報（例えば、第一秘密鍵格納部１２０３の秘密鍵と第二秘密鍵格納部１２１３の公開鍵）を保持してもよい。

【００７０】

（４）第一秘匿通信処理部１２０４

第一秘匿通信処理部１２０４は、読取部１２０１から配布データ領域特定情報ＡＲＥＡが入力された場合、まず、第一秘密鍵格納部１２０３に格納されている共通秘密鍵ＳＫを取得する。そして、共通秘密鍵ＳＫを基に配布データ領域特定情報ＡＲＥＡの暗号化を行い、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを生成する。そして、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを第二秘匿通信処理部１２１４へ出力する。暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、第二秘匿通信処理部１２１４と同じ暗号アルゴリズムを用いる。なお、例えば、非特許文献１に記載のチャレンジレスポンス認証方式を用いて、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを第二秘匿通信処理部１２１４へ出力する前に、出力先である第二秘匿通信処理部１２１４の正当性を認証するようにしてもよい。また、例えば、非特許文献３に記載の鍵共有方法（Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌｓ）を用いて、第二秘匿通信処理部１２１４と毎回異なるセッション鍵ＳＥＫを共有し、そのセッション鍵ＳＥＫを基に、配布データ領域特定情報ＡＲＥＡを暗号化して、第二秘匿通信処理部１２１４へ出力してもよい。

【００７１】

（５）デバイス鍵格納部１２１１

デバイス鍵格納部１２１１は、配布センタ１０の実行装置情報格納部１００３の中の鍵情報の一部を保持するものであり、デバイス鍵格納部１２１１に与えられる鍵情報と暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫが取得出来るものである。例えば、実行装置情報格納部１００３が図３のような場合、デバイス鍵格納部１２１１には、装置識別子ＡＩＤｉとデバイス鍵Ｋｉ（ｉは１からｓのいずれか）が与えられる。

【００７２】

（６）コンテンツ鍵取得部１２１２

コンテンツ鍵取得部１２１２は、読取部１２０１から暗号化鍵束ＫＢが入力された場合、デバイス鍵格納部１２１１に格納されている鍵情報及び暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫを取得する。例えば、暗号化鍵束ＫＢが図４のような場合で、デバイス鍵格納部１２１１には装置識別子ＡＩＤｉとデバイス鍵ＤＫｉ（ｉは１からｓのいずれか）が与えられている場合、コンテンツ鍵取得部１２１２はデバイス鍵格納部１２１１から装置識別子ＡＩＤｉとデバイス鍵ＤＫｉを取得し、暗号化鍵束ＫＢの中から装置識別子ＡＩＤｉに対応する暗号化コンテンツ鍵ＥＮＣＣＫｉ（ＥＮＣＣＫ１からＥＮＣＣＫｓの何れか）を取得する。そしてデバイス鍵ＤＫｉを基に、暗号化コンテンツ鍵ＥＮＣＣＫｉを復号化することによって、コンテンツ鍵ＣＫ＝Ｄｅｃ（ＤＫｉ、ＥＮＣＣＫｉ）を取得する。なお、Ｄｅｃ（Ｋ、Ｃ）は暗号文Ｃを復号化鍵Ｋを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵ＣＫを実行部１２１７へ出力する。

【００７３】

（７）第二秘密鍵格納部１２１３

第二秘密鍵格納部１２１３は、第二秘匿通信処理部１２１４と第一秘匿通信処理部１２

０４との間で秘匿通信を行うための鍵情報を保持するものであり、予め与えられる１２８ビットの鍵情報である共通秘密鍵ＳＫを保持する。与えられる共通秘密鍵ＳＫの値は、第一秘密鍵格納部１２０３が保持する共通秘密鍵ＳＫの値と同じである。なお、第二秘密鍵格納部１２１３は、共通秘密鍵ＳＫではなく、公開鍵暗号用の鍵情報（例えば、第二秘密鍵格納部１２１３の秘密鍵と第一秘密鍵格納部１２０３の公開鍵）を保持してもよい。

【００７４】

（８）第二秘匿通信処理部１２１４

第二秘匿通信処理部１２１４は、第一秘匿通信処理部１２１４から暗号化配布データ領域特定情報ＥＮＣＡＲＥＡが入力された場合、まず、第二秘密鍵格納部１２１３に格納されている共通秘密鍵ＳＫを取得する。そして、共通秘密鍵ＳＫを基に配布データ領域特定情報ＡＲＥＡの復号化を行い、配布データ領域特定情報ＡＲＥＡを生成する。そして、配布データ領域特定情報ＡＲＥＡを認証情報検証部１２１６へ出力する。暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、第一秘匿通信処理部１２０４と同じ暗号アルゴリズムを用いる。なお、例えば、非特許文献１に記載のチャレンジレスポンス認証方式を用いて、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを第一秘匿通信処理部１２０４から入力される前に、入力元である第一秘匿通信処理部１２０４の正当性を認証するようにしてもよい。また、例えば、非特許文献３に記載の鍵共有方法（Ｋｅｙ　Ａｇｒｅｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌｓ）を用いて、第一秘匿通信処理部１２０４と毎回異なるセッション鍵ＳＥＫを共有し、そのセッション鍵ＳＥＫを基に、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを復号化して、認証情報検証部１２１６へ出力してもよい。

【００７５】

（９）検証情報格納部１２１５

検証情報格納部１２１５は、認証情報ＡＵＴＨの正当性を検証するために必要な検証情報ＶＥＲを保持するものである。この検証情報ＶＥＲに対応する認証情報生成情報ＧＥＮＡＵＴＨは、配布センタ１０の認証情報生成情報格納部１００９に格納されている。例えば、検証情報ＶＥＲはデジタル署名アルゴリズムの署名検証鍵（公開鍵）である。

【００７６】

（１０）認証情報検証部１２１６

認証情報検証部１２１６は、読取部１２０１からコンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨが入力され、第二秘匿通信処理部１２１４から配布データ領域特定情報ＡＲＥＡが入力された場合、認証情報ＡＵＴＨの正当性を検証する。検証は以下のように行われる。

【００７７】

まず、図１６で一例を示すように、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎとユニット数ＮＵＭＵ＃１、・・・、ＮＵＭＵ＃ｎから、ｉ組（ｉは１以上ｎ－１以下の自然数）の特定情報とユニット数を選択する。ここで、選択されたｉ組の特定情報とユニット数からなるデータを被選択コンテンツ位置情報とする。ここでは、第三者によってどの特定情報とユニット数が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、認証情報検証部１２１６が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献２が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、認証情報検証部１２１６が温度センサや湿度センサを有することにより実現出来る。

【００７８】

続いて、図１７で示すように、選択されたｉ組の特定情報とユニット数（被選択コンテンツ位置情報）、及び、可搬媒体１１に記録されている第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部を基に、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する。入

替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する方法は、以下の通りである。まず、選択されたｉ組の特定情報とユニット数のそれぞれに対応するｉ個の入替第一ハッシュテーブルを生成する。ここでは、選択されたｉ組の特定情報とユニット数のうち、１組が特定情報ＡＤＤＲ＃１とユニット数ＮＵＭＵ＃１である場合を例に挙げ、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１を生成する手順について説明する。なお、他の特定情報とユニット数の場合であっても、同様の手順となる。まず、ユニット数ＮＵＭＵ＃１を基に、特定情報ＡＤＤＲ＃１に対応する暗号化部分コンテンツＥＮＣＣＮＴ＃１に含まれるユニットの数を認識し、１番目からｄ番目（ｄはユニット数ＮＵＭＵ＃１）までのユニットのうち、ｊ個（ｊは１以上ｍ以下の自然数）のユニットを選択する。ここでも、第三者によってどのユニットが選択されるか推測できないようにする。この方法は、先ほど、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報とユニット数から、ｉ組の特定情報とユニット数を選択する方法と同様の方法が利用可能であるため、説明を省略する。以後、説明を簡略化するために、ｊは１とし、図１８で示すように、ユニットＵ＃３（図１８における横点線）が選択されたとする。そして、そのユニットＵ＃３に対する属性値である第一ハッシュ値Ｈ１（図１８における縦線）を計算する。また、特定情報ＡＤＤＲ＃１及びユニット数ＮＵＭＵ＃３を基に、読取部１２０１経由で可搬媒体１１からＩＤ１＃３以外の選択されなかった第一識別子に対応する第一ハッシュ（図１８における横点線）を取得する。そして、選択された第一識別子に対応するユニットの属性値を計算することによって取得した第一ハッシュ値、及び、選択されなかった第一識別子に対応する第一ハッシュ値から構成される、図１８で示される、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１を生成する。

【００７９】

続いて、生成されたｉ個の入替第一ハッシュテーブル、及び、可搬媒体１１に記録されている第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部を基に、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する方法について説明する。図１９で一例を示すように、まず、ｉ個の入替第一ハッシュテーブルのそれぞれに対する属性値として、第二ハッシュ値（図１９における縦線）を生成する。図１９では、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１に対する属性値として第二ハッシュ値Ｈ２＃１、・・・、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃ｃに対する属性値として第二ハッシュ値Ｈ２＃ｃとしている。次に、選択されなかった特定情報に対応する第二ハッシュ値を、読取部１２０１経由で可搬媒体１１から取得する（図１９における横点線）。そして、入替第一ハッシュテーブルの属性値を計算することによって取得した第二ハッシュ値、及び、選択されなかった特定情報に対応する第二ハッシュ値から構成される、図１９で示される、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する。

【００８０】

最後に、検証情報格納部１２１５に格納されている検証情報ＶＥＲを使って、図２０で示すように、認証情報ＡＵＴＨが発行センタ１０による入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳ及び配布データ領域特定情報ＡＲＥＡに対する正規の認証情報であるかを検証する。例えば、まず、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とｎ個の特定情報と、コンテンツ位置情報ＰＯＳに含まれるｎ個の特定情報とｎ個のユニット数から、第二ハッシュ値と特定情報とユニット数のｎ組を生成し、デジタル署名検証アルゴリズムを用いて、認証情報ＡＵＴＨがそれらの値と配布データ領域特定情報ＡＲＥＡを結合した値｛ＨＡＳＨ２＃１｜｜ＡＤＤＲ＃１｜｜ＮＵＭＵ＃１｝｜｜｛ＨＡＳＨ２＃２｜｜ＡＤＤＲ＃２｜｜ＮＵＭＵ＃１｝｜｜・・・｜｜｛ＨＡＳＨ２＃ｎ｜｜ＡＤＤＲ＃ｎ｜｜ＮＵＭＵ＃ｎ｝｜｜ＡＲＥＡに対する正規のデジタル署名であるかどうか検証する。このデジタル署名検証アルゴリズムは、配布センタ１０の認証情報生成部１０１０で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。認証情報検証部１２１６は、認証情報ＡＵＴＨが発行センタ１０による正しい認証情報である場合にのみ、実行開始許可情報

ＰＥＲＭを実行部１２１７へ出力する。なお、被選択コンテンツ位置情報に含まれるｉ個の特定情報に対応するｉ個の暗号化部分コンテンツを、被選択部分コンテンツとする。なお、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎとユニット数ＮＵＭＵ＃１、・・・、ＮＵＭＵ＃ｎから、ｉ組の特定情報とユニット数を選択する際、同じ特定情報とユニット数の組を重複して選択するようにしてもよい。なお、選択したｉ組の特定情報とユニット数の各組に対して、それぞれ異なるユニットの数（ｊ）を選択するようにしてもよい。

【００８１】

（１１）実行部１２１７

実行部１２１７は、コンテンツ鍵取得部１２１２からコンテンツ鍵ＣＫが入力され、かつ、認証情報検証部１２１６から実行開始許可情報ＰＥＲＭが入力された場合に、読取部１２０１経由で、可搬媒体１１に記録されている暗号化コンテンツＥＮＣＣＮＴを逐次取得し、逐次コンテンツ鍵ＣＫを基に復号化を行って、逐次実行するものである。例えば、実行部１２１７はＭＰＥＧ２データやＭＰ３データをデコードする機能を有するデコータを有していて、ＭＰＥＧ２形式の動画コンテンツやＭＰ３形式の音声コンテンツであるコンテンツＣＮＴを逐次デコードして、外部に出力するものである。また、例えば、実行部１２１７は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生するようなものでも良いし、別の可搬媒体や記録媒体にコンテンツデータを出力するようなものでも良いし、印刷機能を有しコンテンツデータを紙などに印刷するようなものでもよい。

【００８２】

＜実行装置１２の動作＞

以上で、実行装置１２の構成について説明を行ったが、ここで実行装置１２の動作について、図２１に示すフローチャートを用いて説明する。なお、実行装置１２の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【００８３】

実行装置１２が可搬媒体１１のデータを読み取り可能になった場合に、読取部１２０１は可搬媒体１１に記録されている配布データ領域特定情報ＡＲＥＡを取得し、配布データ領域特定情報ＡＲＥＡを配布データ領域特定情報格納部１２０２に格納する。そして、配布データ領域特定情報ＡＲＥＡを第一秘匿通信処理部１２０４へ出力する。（ステップＳ１２１）

読取部１２０１は可搬媒体１１に記録されている暗号化鍵束ＫＢ及びコンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨを取得し、暗号化鍵束ＫＢをコンテンツ鍵取得部１２１２へ出力し、コンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨを認証情報検証部１２１６へ出力する。（ステップＳ１２２）。

【００８４】

配布データ領域特定情報ＡＲＥＡが入力された第一秘匿通信処理部１２０４は、第一秘密鍵格納部１２０５が保持する秘密共有鍵ＳＫを基に配布データ領域特定情報ＡＲＥＡを暗号化し、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを取得し、暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを第二秘匿通信処理部１２１４へ出力する。（ステップＳ１２３）

暗号化鍵束ＫＢを入力されたコンテンツ鍵取得部１２１２は、デバイス鍵格納部１２１１が保持している鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫを実行部１２１７へ出力する。（ステップＳ１２４）

暗号化配布データ領域特定情報ＥＮＣＡＲＥＡが入力された第二秘匿通信処理部１２１４は、第二秘密鍵格納部１２１５が保持する秘密共有鍵ＳＫを基に暗号化配布データ領域特定情報ＥＮＣＡＲＥＡを復号化し、配布データ領域特定情報ＡＲＥＡを取得し、配布データ領域特定情報ＡＲＥＡを認証情報検証部１２１６へ出力する。（ステップＳ１２５）

コンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡと認証情報ＡＵＴＨを入

力された認証情報検証部１２１６は、コンテンツ位置情報ＰＯＳを基に、可搬媒体１１に記録されている第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部を用いて入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する。（ステップＳ１２６）

認証情報検証部１２１６は、検証情報格納部１２１５に格納されている検証情報ＶＥＲを使って、認証情報ＡＵＴＨが発行センタ１０によるコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡと入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の認証情報であるかを検証する。（ステップＳ１２７）

認証情報検証部１２１６は、認証情報ＡＵＴＨが発行センタ１０による正しい認証情報である場合にのみ、実行開始許可情報ＰＥＲＭを実行部１２１７へ出力し、ステップＳ１２９へ進む。もし、認証情報ＡＵＴＨが正しい認証情報ではない場合、処理を終了する。（ステップＳ１２８）

コンテンツ鍵ＣＫ及び実行開始許可情報ＰＥＲＭを入力された実行部１２１７は、読取部１２０１経由で、可搬媒体１１に記録されている暗号化コンテンツＥＮＣＣＮＴを逐次取得し、逐次コンテンツ鍵ＣＫを基に復号化を行って、逐次実行する。ここで、実行部１２１７から可搬媒体１１に記録されているデータの読取要求が来た読取部１２０１は、配布データ領域特定情報格納部１２０２に格納されている配布データ領域特定情報ＡＲＥＡを取得し、実行部１２１７から読取要求が来たデータが配布データ領域特定情報ＡＲＥＡで識別される記録領域内であれば、可搬媒体１１に記録されているデータを取得して、実行部１２１７に出力するようにする。（ステップＳ１２９）

以上が、不正コンテンツ検知システム１の構成要素である実行装置１２の構成と動作である。尚、配布データ領域特定情報格納部１２０２、第一秘密鍵格納部１２０３、第一秘匿通信処理部１２０４、等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。同様に、デバイス鍵格納部１２１１、コンテンツ鍵取得部１２１２、第二秘密鍵格納部１２１３、第二秘匿通信処理部１２１４、検証情報格納部１２１５、認証情報検証部１２１６、実行部１２１７等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。

【００８５】

ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサー を利用しても良い。

【００８６】

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム１の効果＞

以上、不正コンテンツ検知システム１について実施の形態に基づいて説明したが、この不正コンテンツ検知システム１においては、配布センタ１０は、著作権者によって可搬媒体１１に記録されたデータのデータ領域の領域である配布データ領域特定情報ＡＲＥＡを記録するようにして、実行装置１２では、その配布データ領域特定情報ＡＲＥＡで指定されたデータ領域の領域外にあるデータは取得しないようにした。実施の形態において、配布データ領域特定情報は、可搬媒体１１に記録されているデータの開始物理アドレスと最終物理アドレスの組である。このことにより、実行装置１２では配布データ領域特定情報ＡＲＥＡにより予め著作権者によって指定された領域外のデータは取得しないため、不正コンテンツを実行、再生出来ないようになる。また可搬媒体１１には、さらに、配布データ領域特定情報ＡＲＥＡに対する認証情報ＡＵＴＨを記録するようにして、実行装置１２

では、認証情報ＡＵＴＨが可搬媒体１１に記録された配布データ領域特定情報ＡＲＥあに対する正規の著作権者の認証情報であるか検証し、検証が成功した場合にのみ、コンテンツＣＮＴの実行、再生を行うようにした。このことにより、著作権を保持しない不正者が、可搬媒体１１の記録されている配布データ領域特定情報ＡＲＥＡを改ざんしたとしても、その可搬媒体１１に記録されているコンテンツは実行、再生しないようになった。このことにより、上記で示したような不正行為に対する耐性を向上させることが出来る。

【００８７】

また、実行装置１２において、配布された不正コンテンツが実行、再生される不正行為の別の一形態として、可搬媒体１１に記録されているデータを読み出すドライブ部１２０と、ドライブ部１２０によって取得されたデータを実行、再生するコンテンツ実行部１２１との間に流れるデータを改竄される場合がある。そこで、ドライブ部１２０からコンテンツ実行部１２１へ出力するデータの一部（例えば、配布データ領域特定情報ＡＲＥＡ）を暗号化して出力するようにした。これにより、不正者は、ドライブ部１２０が出力したデータを別のデータに差し替えてコンテンツ実行部１２１へ出力しようとしても、不正者は正しく暗号化することが出来ないため、正しくコンテンツ実行部１２１へ出力できなくなった。この際、同じデータであっても、ドライブ部からコンテンツ実行部へ出力する暗号文が異なるようにしてもよい。これは、例えば、ドライブ部１２０とコンテンツ実行部１２１が毎回異なるセッション鍵を共有することにより実現出来る。このことにより、著作権を保持しない不正者によって不正コンテンツが実行、再生されるという不正行為を防ぐことが出来るようになった。

＜変形例＞

上記に説明した実施の形態は、本発明の実施の形態の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【００８８】

（１）本発明は、上記に示す実行装置１２のコンテンツ実行部１２１の動作を、図２２で例を示すようなドライブ部を有するコンピュータにより実現するコンピュータプログラムであるとしてもよい。さらには、前記コンピュータプログラムからなるデジタル信号であるとしても良い。

（２）上記で説明した実施の形態は、本発明の不正コンテンツ検知システムの一実施形態にすぎない。本発明の効果を得るために、以下の動作のみで十分であることを補足しておく。まず、配布センタ１０は、実行装置１２へ配布するコンテンツＣＮＴの領域を特定する配布データ領域特定情報ＡＲＥＡ（例えば、開始物理アドレスと最終物理アドレスの組）を生成し、その配布データ領域特定情報ＡＲＥＡを含む検証対象データに対する認証情報ＡＵＴＨを生成し、コンテンツＣＮＴと配布データ領域特定情報ＡＲＥＡと認証情報ＡＵＴＨを実行装置１２へ配布する。実行装置１２は、配布データ領域特定情報を基に認証情報を検証し、検証結果が正当な場合にのみ、配布データ領域特定情報を基に配布データを特定し、その配布データのみをコンテンツとして実行、もしくは再生する。これにより、本発明の効果は得ることが出来る。

【００８９】

（３）実施の形態１では、不正者によってドライブ部１２０が出力したデータを別のデータに差し替えて正しくコンテンツ実行部１２１へ出力出来ないようにすることを目的に、配布データ領域特定情報ＡＲＥＡだけを暗号化していたが、これに限るものではない。例えば、ドライブ部１２０がコンテンツ実行部１２１へ出力するデータを全て暗号化するようにしてもよい。もしくは、ドライブ部１２０がコンテンツ実行部１２１へ出力する配布データ領域特定情報ＡＲＥＡ以外のデータ（例えば、暗号化鍵束、第一ハッシュテーブル群、第二ハッシュテーブル、コンテンツ位置情報、認証情報、暗号化コンテンツの全部もしくは一部のデータ）を暗号化するようにしてもよい。もしくは、ドライブ部１２０がコンテンツ実行部１２１へ出力するデータを全く暗号化しないようにしてもよい。

【００９０】
（４）実施の形態１の可搬媒体１１に記録されている配布データ領域特定情報ＡＲＥＡは、可搬媒体１１に記録されているデータの領域を識別するものだけに限るものではない。一例として、例えば、配布データ領域特定情報ＡＲＥＡは、可搬媒体１１に記録されているデータの最終物理アドレスだけでもよい。もしくは、可搬媒体１１に記録されているデータの開始物理アドレスだけでもよい。もしくは、可搬媒体１１に記録されているデータの総サイズであってもよい。例えば、配布センタ１０は、可搬媒体１１に記録するデータの総サイズを配布データ領域特定情報ＡＲＥＡとして生成し、その配布データ領域特定情報ＡＲＥＡを可搬媒体１１に記録する。そして、実行装置１２の読取部１２０１では、可搬媒体１１に記録された配布データ領域特定情報ＡＲＥＡを取得する。その後、読取部１２０１は、可搬媒体１１から取得したデータの総サイズを計測する。そして、読取部１２０１は、可搬媒体１１から取得したデータの総サイズが、可搬媒体１１に記録された配布データ領域特定情報ＡＲＥＡで識別されるサイズよりも多くなった場合、以後読取部１２０１は、可搬媒体１１からデータを取得しないようにする。これにより、著作権を保持しない不正者により、新たな可搬媒体に、正規の配布センタによって配布された可搬媒体のデータをそのまま記録して、新たな可搬媒体においてまだ記録可能な領域に不正コンテンツを記録された場合でも、読取部１２０１は予め著作権者によって指定されたデータの総サイズ以上は取得しないため、そのような不正行為を防止することが出来る。
【００９１】
（５）実施の形態１の配布センタ１０は、図２で示すような構成に限るものではない。例えば、図２３で示すように、認証情報ＡＵＴＨを生成する認証情報生成部１０１０は発行センタが行うようにしても良い。この場合、発行センタは、例えば、正規の著作権者であり、可搬媒体１１へ記録するのは、例えば、ディスク製造業者（プレス業者）などである。
【００９２】
（６）実施の形態１のコンテンツＣＮＴは、動画データや音声データなどのコンテンツであったが、これに限るものではない。例えば、コンテンツは画像コンテンツでもよいし、テキストコンテンツでもよい。また、コンピュータプログラムであっても良い。この場合、実行装置１２は、コンピュータプログラムを実行するために必要なＣＰＵやメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置１２では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。
【００９３】
（７）実施の形態１において、可搬媒体１１に記録されるデータは、図１４のような順番で記録されていなくてもよい。
（８）実施の形態１において、可搬媒体１１には、暗号化コンテンツＥＮＣＣＮＴ以外の第二コンテンツＣＮＴ２を記録するようにしても良い。そして、暗号化コンテンツＥＮＣＣＮＴの検証処理を行っている間に、その第二コンテンツＣＮＴ２を実行、再生するようにしてもよい。例えば、その第二コンテンツＣＮＴ２の例としては、映画のオープニング画面やＤＶＤのメニュー画面、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面などが挙げられる。なお、第二コンテンツＣＮＴ２は、予め実行装置１２内に格納されていても良い。
【００９４】
（９）実施の形態１において、可搬媒体１１に記録されている暗号化コンテンツＥＮＣＣＮＴの検証処理を行っている間に、配布センタ１０によって許諾された暗号化コンテンツＥＮＣＣＮＴのある一部分を実行、再生するようにしてもよい。例えば、その暗号化コンテンツＥＮＣＣＮＴのある一部分の例としては、映画のオープニング画面やＤＶＤのメニュー画面、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面などが挙げられる。
【００９５】

（１０）実施の形態１において、暗号化部分コンテンツの属性値（ハッシュ値）は２層構造であってが、これに限るものではない。例えば、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、認証情報ＡＵＴＨはその第一ハッシュテーブルに対する認証情報としてもよい（１層型）。もしくは、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、第一ハッシュテーブルをグループ分けし、その各グループの第一ハッシュテーブルを連結した値に対する属性値（ハッシュ値）を第二ハッシュテーブルとして、第二ハッシュ値をグループ分けし、その各グループの第二ハッシュ値を連結した値に対する属性値（ハッシュ値）を第三ハッシュテーブルとして、認証情報ＡＵＴＨはその第三ハッシュテーブルに対する認証情報としてもよい（３層型）。もしくは、４層以上の構造にしてもよい。層を深くすることにより、可搬媒体に記録すべき属性値の数は増えるが、実行装置が可搬媒体から取得すべき属性値の数を減らすことが出来る。一方、層を浅くすることにより、実行装置が可搬媒体から取得すべき属性値の数は増えるが、可搬媒体に記録すべき属性値の数を減らすことが出来る。このようにバランスを変えることが出来るようになる。

【００９６】

（１１）実施の形態１の可搬媒体１１において、図２４で示すように、ｎ個の暗号化部分コンテンツの再生、実行手順を記述したデータである実行手順データＮＡＶを記録するようにして、実行装置１２の実行部１２１７では、その実行手順データＮＡＶを基に、ｎ個の暗号化部分コンテンツを再生、実行するようにしてもよい。この場合、配布センタ１０は、その実行手順データＮＡＶを含めたデータに対する認証情報を生成するようにして、実行装置１２では、認証情報によりその実行手順データＮＡＶの正当性が検証された場合にのみ、実行部１２１７へ暗号化コンテンツＥＮＣＣＮＴを実行、再生するようにしてもよい。なお、実行手順データＮＡＶは、例えば、ＤＶＤ－ＶＩＤＥＯ形式におけるナビゲーションファイル（拡張子がＩＦＯのファイル）である。

【００９７】

（１２）実施の形態１において、コンテンツＣＮＴは予めｎ個の部分コンテンツに分割されているとしたが、これに限るものではない。例えば、コンテンツＣＮＴが予めｎ個の部分コンテンツに分割されていない場合、入力部１００１は、ある所定の区切りに従ってコンテンツＣＮＴをｎ個に分割するようにしても良い。この所定の区切りは、予めシステム共通のパラメータとして与えられていても良いし、外部から入力されてもよい。外部から入力される場合、例えば、入力部１００１がキーボードやマウスと接続されていることにより実現できる。所定の区切りは、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位でもよい。また、別の例として、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、ＶＯＢ単位や、ＶＯＢＵ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ　Ｕｎｉｔ）単位、セル（Ｃｅｌｌ）単位などでもよい。コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、例えば、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などでもよい。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（ＥＣＣブロック単位）などでもよい。なお、部分コンテンツのサイズは、全て同じである必要はなく、それぞれ異なっていても良い。また、コンテンツを分割する数（ｎ）は、コンテンツＣＮＴに応じて変えても良い。

【００９８】

（１３）実施の形態１において、実行装置１２の読取部１２０１は、可搬媒体１１から複数のユニットを取得する場合、アクセス時間の高速化を目的に、ユニットを取得する順番を最適化するようにしても良い。

ここでは一例として、以下のような状況を想定する。実行装置１２の読取部１２０１は、４個のユニットＵ＃１、Ｕ＃２、Ｕ＃３、Ｕ＃４を取得したいとする。また、可搬媒体１１は、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの光ディスクであるとする。その可搬媒体１１（光ディスク）上には、データを記録する部分がいくつかに分かれており、年輪状に広がっている各領域をトラックと呼ぶ。各トラックには、いくつかのセクタを含み、データ

はセクタ単位で読み書きされる。例えば、１セクタのサイズは５１２バイトである。このような場合、可搬媒体１１上の読み取り対象データは、トラック識別番号やセクタ識別番号やセクタサイズにより特定することが出来る。読取部１２０１は、ヘッド機構部（ピックアップ）及び回転軸を備え、回転軸により可搬媒体１１（光ディスク）を半時計回りに回転させるものとする。ヘッド機構部（ピックアップ）から特定情報（トラック識別番号やセクタ識別番号やセクタサイズ）を指定することで、対象部分のデータを取得出来るものとする。ここでは、４個のユニットＵ＃１、Ｕ＃２、Ｕ＃３、Ｕ＃４は、図２５のように可搬媒体１１（光ディスク）上の位置に記録されているとし、可搬媒体１１（光ディスク）とヘッド機構部も、図２５で示す場所に存在しているとする。ここで、一般に、該当読取位置に対応するトラック位置へヘッド機構部（ピックアップ）を移動させる時間がかかることが知られている。言い換えると、可搬媒体１１（光ディスク）上における内周のトラックから外周方向への移動、もしくは、外周のトラックから内周方向への移動に大きな処理時間がかかることに起因している。可搬媒体１１（光ディスク）上における内側のトラック上にあるデータを読み込んだ後に、外側のトラック上にあるデータを読み込み、その後、また内側のトラック上にあるデータを読み込む場合がその一例である。

【００９９】

上記のような状況の場合、実施の形態１の動作に沿えば、まず１番目に、ユニットＵ＃１の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後、２番目にユニットＵ＃２の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後も同様に、ユニットＵ＃３の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得し、最後に、ユニットＵ＃４の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。つまり、ユニットＵ＃１を取得するまでに、ヘッド機構部を内周から外周へ移動させ、続いて、ユニットＵ＃２を取得するまでに、ヘッド機構部を外周から内周へ移動させる。その後も、ユニットＵ＃３を取得するまでに、ヘッド機構部を内周から外周へ移動させ、最後に、ユニットＵ＃４を取得するまでに、ヘッド機構部を外周から内周へ移動させる。つまり、４つのデータを取得するまでに、ヘッダ機構部を何度も移動往復させる必要があることが分かる。

【０１００】

そこで、本変形例では、上記全４つのデータの取得時間を短くする目的で、実行装置１２の読取１２０１は、まずはじめに、それぞれのデータを取得する順序の最適値を計算する。例えば、一番初めに一番内側のトラック上にあるデータを全て取得して、その次に、一つ外側のトラック上にあるデータを全て取得いく、というようなことを繰り返す。この場合、トラック上に一つもデータがない場合は、そのトラックをスキップして次のトラックに進むようにする。例えば、４つのユニットが図２５のように可搬媒体１１（光ディスク）上の位置に記録されているとし、さらに、可搬媒体１１（光ディスク）及びヘッド機構部（ピックアップ）が図２５で示す場所に存在しているとする。すると、このデータを取得する順序の最適値は、内周側から外周側に向かって、ユニットＵ＃２、ユニットＵ＃４、ユニットＵ＃３、ユニットＵ＃１となる。このようにすることで、可搬媒体１１（光ディスク）上に記録されているとびとびの部分データをランダムに取得する（いわゆるランダムアクセス）場合にでも、取得したい全てのデータを取得するまでの時間を短縮することが出来る。なお、当然、ユニットは４個以外であっても適用可能である。

【０１０１】

なお、最適化手段は、読取部１２０１（ヘッド機構部や回転軸等）の動作の特徴に依存するため、本変形例で説明した最適化手段は、あくまで一例であることを注意しておく。例えば、光ディスクの回転制御方式には、角速度一定方式や線速度一定方式があり、これらの特徴を考慮するようにしても良い。また、可搬媒体１１は当然光ディスクでなくてもよく、例えばハードディスクなどでも同様のことが実現出来る。

【０１０２】

（１４）実施の形態１において、認証情報検証部１２１６は、予め与えられているパラ

メータｉ、ｊに従って検証を実施していたが、これに限るものではない。例えば、配信装置１０は可搬媒体１１に、パラメータｉ、ｊの両方もしくは片方を記録するようにして、実行装置１２は可搬媒体１１に記録されているパラメータｉ、ｊの両方もしくは片方に従って検証するようにしてもよい。この場合、配布センタ１０は、そのパラメータｉ、ｊの両方（もしくは片方）を含めたデータに対する認証情報を生成するようにして、実行装置１２では、認証情報によりそのパラメータｉ、ｊの両方（もしくは片方）の正当性が検証された場合にのみ、実行部１２１７へ暗号化コンテンツＥＮＣＣＮＴを実行、再生するようにしてもよい。このパラメータｉ、ｊは、多くすればセキュリティは向上するが、処理時間が多くなり、少なくすれば処理時間は少なくなるが、セキュリティは低下するという特徴を有する。つまり、本変形例を用いることで、著作権者（コンテンツ配布者）の要望やポリシーに依存して、セキュリティレベルなどを設定することが出来るようになる。なお、実行装置１２において、可搬媒体１１にパラメータｉ、ｊが記録されていない場合、予め与えられるデフォルトのパラメータｉ、ｊを用いるようにしても良い。

【０１０３】

（１５）実施の形態１において、コンテンツ位置情報ＰＯＳは、ｎ個の暗号化部分コンテンツの構成、及び、暗号化部分コンテンツの中のユニットの構成を特定出来るものであれば、どのようなものでもよい。例えば、特定情報は、暗号化部分コンテンツを識別する光ディスク上の先頭の論理アドレスとオフセット（データサイズ）でもよい。もしくは、先頭の論理アドレスと終端の論理アドレスであっても良い。もしくは、先頭の物理アドレスとオフセット（データサイズ）であっても良い。もしくは、先頭の物理アドレスと終端の物理アドレスであっても良い。さらに、ユニット数は、各ユニットの先頭の論理アドレスとデータサイズの羅列であってもよい。もしくは、先頭と終端の論理アドレスの羅列であってもよい。もしくは、先頭の物理アドレスとデータサイズの羅列であってもよい。もしくは、先頭と終端の物理アドレスの羅列であっても良い。

【０１０４】

また、コンテンツ位置情報ＰＯＳにおいて、各特定情報に対応する暗号化部分コンテンツに含まれるユニット数が同じ場合、図２６で示すとおり、ｎ個のユニット数の替わりに１つの共通ユニット数ＡＬＬＮＵＭＵ（一つの第二ハッシュ値が、いくつの第一ハッシュ値から計算されているかを示す属性値比率）がコンテンツ位置情報ＰＯＳに含まれていても良い。この場合、認証情報ＡＵＴＨは、図２７で示すように、第二ハッシュテーブルＨＡＳＨＴＢＬ２及び共通ユニット数ＡＬＬＮＵＭＵを連結した値に対する認証情報として、実行装置１２における検証時には、図２８で示すように、認証情報ＡＵＴＨが入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２及び共通ユニット数ＡＬＬＮＵＭＵを連結した値に対する正しい認証情報であるか検証するようにしても良い。

【０１０５】

（１６）実施の形態１の認証情報ＡＵＴＨは、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡとを連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳと配布データ領域特定情報ＡＲＥＡに加え、コンテンツ鍵ＣＫを連結した値に対する認証情報であっても良い。こうすることにより、コンテンツ鍵ＣＫを持たないものは、認証情報ＡＵＴＨの正当性を検証出来なくなり、安全性がより高まる。また、例えば、第二ハッシュテーブルＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とコンテンツ位置情報ＰＯＳに含まれるｎ個の特定情報とｎ個のユニット数と配布データ領域特定情報ＡＲＥＡを連結した値に対する認証情報であっても良い。また、第二ハッシュテーブルＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とコンテンツ位置情報ＰＯＳに含まれるｎ個のユニット数と配布データ領域特定情報ＡＲＥＡの値を連結した値に対する認証情報であっても良い。

【０１０６】

（１７）実施の形態１の可搬媒体１１では、コンテンツＣＮＴは暗号化されて記録されていたが、可搬媒体１１にはコンテンツＣＮＴをそのまま記録するようにしても良い。こ

うすることにより、実行装置１２で暗号化コンテンツＥＮＣＣＮＴを復号化する必要がなくなるという効果が生まれる。

（１８）実施の形態１の実行装置１２のコンテンツ鍵取得部１２１２では、暗号化鍵束ＫＢ、及びデバイス鍵格納部１２１１に格納されている情報を用いて、コンテンツ鍵ＣＫを取得していたが、配布センタ１０がデバイス鍵格納部１２１１の替わりに、コンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部１２１２はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ１０は可搬媒体１１に暗号化鍵束ＫＢを記録する必要はなく、実行装置１２は暗号化鍵束ＫＢを受信する必要もない。こうすることにより、可搬媒体１１に暗号化鍵束ＫＢを記録しなくてすむため、記録データのサイズを削減することが出来る。

【０１０７】

（１９）実施の形態１の配布センタ１０は、可搬媒体１１を介して実行装置１２へコンテンツＣＮＴを配布していたが、これに限るものではない。例えば、配布センタ１０と実行装置１２がインターネット等の通信ネットワークに接続されており、配布センタ１０は、その通信ネットワークを介して実行装置１２へコンテンツＣＮＴを配布するようにしてもよい。もしくは、放送網を介して配布してもよい。

【０１０８】

（２０）実施の形態１の配布センタ１０の認証情報生成情報格納部１００９、及び、実行装置１２の検証情報格納部１２１５は、これに限るものではない。例えば、以下のような例が考えられる。

（ｉ）認証情報生成情報格納部１００９は、図２９で示すように、１つの認証情報生成情報ＧＥＮＡＵＴＨｉ（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗのいずれか（ｗは１以上の自然数））と対応する検証情報識別子ＶＥＲＩＤｉを保持しており、検証情報格納部１２１５は、図３０で示すように、ｗ組の検証情報識別子（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗ）と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報（ＶＥＲ１、・・・、ＶＥＲｗ）を保持する。配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報識別子ＧＥＮＡＵＴＨｉを記録するようにして、実行装置１２の認証情報検証部１２１６は、可搬媒体１１に記録されている検証情報識別子ＧＥＮＡＵＴＨｉに対応する検証情報ＶＥＲｉ（ＶＥＲ１、・・・、ＶＥＲｗのいずれか）を検証情報格納部１２１５から取得し、その検証情報ＶＥＲｉを基に、認証情報ＡＵＴＨを検証するようにしてもよい。

【０１０９】

（ｉｉ）認証情報生成情報格納部１００９には、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲを保持しており、検証情報格納部１２１５は何も保持してない。配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報ＶＥＲを加えて記録するようにして、実行装置１２の認証情報検証部１２１６は、可搬媒体１１に記録されている検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証する。

【０１１０】

（ｉｉｉ）認証情報生成情報格納部１００９には、図３１で示すように、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲ、及び、第三者機関によって生成された検証情報ＶＥＲに対する認証情報（例えばデジタル署名）であるセンタ認証情報ＣＡＵＴＨを保持しており、検証情報格納部１２１５は、図３２で示すように、第三者機関の検証情報であるセンタ検証情報ＣＶＥＲ（例えばデジタル署名の署名検証鍵）を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）や、鍵配布センタなどである。この場合、配布センタ１０の記録部１０１１は、可搬媒体１１に、認証情報生成情報格納部１００９に格納されている検証情報ＶＥＲ及びセンタ認証情報ＣＡＵＴＨを記録するようにして、実行装置１２の認証情報検証部１２１６は、検証情報格納部１２１５のセンタ検証情報ＣＶＥＲを用いて、可搬媒体１１に記録されているセンタ認証情報ＣＡＵＴＨが、検証情報ＶＥＲに対

する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証する。

【０１１１】

これにより、配布センタ１０が複数存在している場合にそれぞれの配布センタ１０に別の検証情報を設定したとしても、実行装置１２に予め各検証情報を保持しておく必要がなくなる。さらに、偽の認証情報が出回った場合にも、どの配布センタ１０から漏洩したのか追跡することが出来る。

（２１）変形例（２０）において、実行装置１２は、さらに、無効検証情報を外部から受信するようにしてもよい。例えば、変形例（２０）の（ｉ）の場合、無効検証情報には、検証情報識別子が含まれており、実行装置１２には、外部から無効検証情報として検証情報識別子ＧＥＮＡＵＴＨｊを受信した場合に、検証情報格納部１２１５に格納されている検証情報識別子ＧＥＮＡＵＴＨｊに対応する検証情報ＶＥＲｊを無効化する検証情報無効化部を備えていてもよい。

【０１１２】

また、変形例（２０）の（ｉｉ）及び（ｉｉｉ）の場合、無効検証情報には、検証情報が含まれており、実行装置１２の検証情報格納部１２１５は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部１２１６は、検証情報格納部１２１５の無効検証情報に、可搬媒体１１に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツＣＮＴの再生、実行開始を行わないようにしてもよい。

【０１１３】

なお、実行装置１２が外部から無効検証情報を受信する方法としては、可搬媒体１１や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。これにより、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。

【０１１４】

（２２）変形例（２１）において、実行装置１２は、最新の無効検証情報のみを検証情報格納部１２１５に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置１２は、検証情報格納部１２１５が保持する無効検証情報よりも発効日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２１５に上書きするようにしてもよいし、また、無効検証情報には発行ＩＤが記載されており、実行装置１２は、検証情報格納部１２１５が保持する無効検証情報よりも発行ＩＤが最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２１５に上書きするようにしてもよい。

【０１１５】

（２３）実施の形態１の実行装置１２は、可搬媒体１１内のコンテンツＣＮＴを再生、実行開始する前に、そのコンテンツＣＮＴが不正なものであるか検証していたが、それに限るものではない。例えば、可搬媒体１１が光ディスクであり、実行装置１２がディスクトレイを有している場合、可搬媒体１１が実行装置１２のディスクトレイに挿入された場合に、そのコンテンツＣＮＴが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体１１内のコンテンツＣＮＴをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時１度しか検証しないですむようになるため、コンテンツＣＮＴの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体１１がＳＤカード等の外部メモリで、実行装置１２が外部メモリスロットを有している場合にも、同様のことが実現出来る。

【０１１６】

（２４）実施の形態１の実行装置１２の認証情報検証部１２１６においては、入替第二ハッシュテーブルを生成し、それを基に認証情報ＡＵＴＨの正当性を検証していたが、こ

れに限るものではない。例えば、実行装置１２の認証情報検証部１２１６では、まず第一ステップとして、図３３で示すように、可搬媒体１１に記録されていた認証情報ＡＵＴＨが、同じく可搬媒体１１に記録されていた第二ハッシュテーブル及びコンテンツ位置情報及び配布データ領域特定情報を結合した値に対する正規の認証情報であるか検証する。次に第二ステップとして、図３４で示すように、選択された特定情報に対応する暗号化部分コンテンツの属性値が、特定情報に対応する第二ハッシュ値と等しいかどうか検証し、さらに、選択された第一識別子に対応するユニットの属性値が、第一識別子に対応する第一ハッシュ値と等しいかどうか検証するようにしてもよい。これにより、同様にコンテンツの正当性を検証することが出来る。暗号化部分コンテンツの属性値と第二ハッシュ値との検証については、図３５に詳細を示している。また、ユニットの属性値と第一ハッシュ値との検証については、図３６に詳細を示している。

【０１１７】

（２５）実施の形態１において、可搬媒体１１には第一ハッシュテーブル群と第二ハッシュテーブルとコンテンツ位置情報と配布データ領域特定情報と暗号化コンテンツとをそれぞれ一つずつ記録していたが、これに限るものではない。例えば、可搬媒体１１には第一ハッシュテーブル群と第二ハッシュテーブルとコンテンツ位置情報と配布データ領域特定情報と暗号化コンテンツとをｚ組（ｚは２以上の自然数）格納しても良い。このような場合、以下のようなことが実現出来る。例えば、可搬媒体１１が光ディスクであり、実行装置１２はディスクトレイを有しているとする。この場合、可搬媒体１１が実行装置１２のディスクトレイに挿入された時に、ｚ組全てのコンテンツ位置情報からいくつかの特定情報を選択し検証を行うようにする。そして、ｚ個ある暗号化コンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツに対応するコンテンツ位置情報の中からいくつかの特定情報を選択し検証を行うようにする。こうして、可搬媒体１１が実行装置１２のディスクトレイに挿入された場合に一度のみ、多くの数の特定情報の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数の特定情報に対して検証するようにする。これにより、ディスクトレイに挿入された可搬媒体１１内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体１１は光ディスクでなくてもよく、例えばＳＤカード等の外部メモリであっても同様のことが実現出来る。

【０１１８】

（２６）実施の形態１においては、実行装置１２の認証情報検証部１２１６では、検証が成功した場合にのみ、実行部１２１７へ実行許可情報ＰＥＲＭを出力していたが、これに限るものではない。例えば、実行部１２１７は、コンテンツ鍵取得部１２１２からコンテンツ鍵を入力された場合に、可搬媒体１１に記録された暗号化コンテンツを逐次取得、復号化、実行もしくは再生するようにして、認証情報検証部１２１６は、検証が失敗した場合に、実行部１２１７へ実行不許可情報ＮＯＴＰＥＲＭを出力するようにして、実行部１２１７は認証情報検証部１２１６から実行不許可情報ＮＯＴＰＥＲＭを入力された場合、実行もしくは再生を停止するようにしてもよい。こうすることにより、コンテンツを実行、再生開始するまでの時間を短縮することが出来るようになる。

【０１１９】

もしくは、実行装置１２の認証情報検証部１２１６は、検証が成功した場合に実行部１２１７へ実行許可情報ＰＥＲＭを出力し、検証が失敗した場合に実行部１２１７へ実行不許可情報ＮＯＴＰＥＲＭを出力するようにしてもよい。さらに、実行不許可情報ＮＯＴＰＥＲＭを入力された実行部１２１７では、外部に不正なコンテンツである旨メッセージを出力（例えば、ディスプレイに「不正なコンテンツです」と表示する）するようにしても良い。実行不許可情報ＮＯＴＰＥＲＭを入力された実行部１２１７では、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を停止するのではなく、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生は通常通り行うが、同時に外部に警告を出力（例えば、ディスプレイに「警告：不正なコンテンツです」と表示する）するようにしても良い。また、実行装置１２とサーバ（配布センタ１０や別のセンタ）とが通信ネットワーク等で接続

されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。また、実行装置１２では以後、あらゆる暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するような状態になってもよい。また、実行装置１２は、不正コンテンツを識別するコンテンツ識別情報（例えば、コンテンツ識別子）を装置内に記録するようにして、一定期間内、もしくは、永久的に、コンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、実行装置１２は、同じコンテンツ識別情報（例えば、コンテンツ識別子）を持つコンテンツがある一定回数以上認証に失敗した場合、一定期間内、もしくは、永久的に、そのコンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、可搬媒体１１が光ディスクであり、実行装置１２がディスクトレイを有している場合、可搬媒体１１がディスクトレイから排出されるようにしても良い。

【０１２０】

（２７）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、ＣＤ、ＭＯ、ＤＶＤ、ＳＤメモリカード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０１２１】

（２８）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０１２２】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人／団体／会社や、正規のディスク製造業者、正規のディスクプレス業者など）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御（例えば警告を表示する、コンテンツの実行／再生を停止する、コンテンツの実行／再生を禁止するなど）することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般、特に記録媒体や可搬媒体（例えば光ディスクやメモリカード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【０１２３】

さらに、本発明は、動画データや音声データなどのマルチメディアコンテンツに限らず、コンテンツの実行順序を制御する実行順序ファイル（ナビゲーションファイル）や、コンピュータプログラム等の保護にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しない等が実現出来る。そのため、安全（セキュア）な処理環境を実現するコンピュータシステム全般、特にＯＳ（Ｏｐｅｒａｔｉｏｎ　Ｓｙｓｔｅｍ）等としても有用である。

【図面の簡単な説明】

【０１２４】

【図１】本発明の実施の形態１における不正コンテンツ検知システムの概要図

【図２】本発明の実施の形態１における配布センタ１０の構成例を示す図

【図３】本発明の実施の形態１における実行装置情報格納部１００３の構成例を示す図

【図４】本発明の実施の形態１における暗号化鍵束ＫＢの一例を示す図

【図５】本発明の実施の形態１における暗号化コンテンツＥＮＣＣＮＴの作成方法の一例を示す図

【図６】本発明の実施の形態１における第一ハッシュテーブル群ＨＡＳＨＴＢＬ１Ｇ及び、第二ハッシュテーブルＨＡＳＨＴＢＬ２の作成方法の一例を示す図

【図７】本発明の実施の形態１における第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１の作成方法の一例を示す図

【図８】本発明の実施の形態１における第二ハッシュテーブルＨＡＳＨＴＢＬ２の作成方法の一例を示す図

【図９】本発明の実施の形態１におけるコンテンツ位置情報ＰＯＳの一例を示す図

【図１０】本発明の実施の形態１における可搬媒体イメージＩＭＧの一例

【図１１】本発明の実施の形態１における認証情報ＡＵＴＨの作成方法の一例を示す図

【図１２】本発明の実施の形態１における第二可搬媒体イメージＩＭＧ２の一例

【図１３】本発明の実施の形態１における配布センタ１０の処理の流れ図（一例）

【図１４】本発明の実施の形態１における可搬媒体１１に記録されるデータの一例

【図１５】本発明の実施の形態１における実行装置１２の構成例を示す図

【図１６】本発明の実施の形態１におけるコンテンツ位置情報ＰＯＳからｉ組の特定情報とユニット数を選択する場合の一例を示す図

【図１７】本発明の実施の形態１における入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の作成方法の一例を示す図

【図１８】本発明の実施の形態１における入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１の作成方法の一例を示す図

【図１９】本発明の実施の形態１における入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の作成方法の一例を示す図

【図２０】本発明の実施の形態１における認証情報ＡＵＴＨの検証方法の一例を示す図

【図２１】実行装置１２の処理の一例を示す流れ図

【図２２】プログラムを処理するコンピュータの例

【図２３】不正コンテンツ検知システムの別の一例

【図２４】可搬媒体１１に記録されるデータの別の一例を示す図

【図２５】可搬媒体１１（光ディスク）と読取部１２０１の一例を示す図

【図２６】コンテンツ位置情報ＰＯＳの別の一例を示す図

【図２７】認証情報ＡＵＴＨの作成方法の別の一例を示す図

【図２８】認証情報ＡＵＴＨの検証方法の別の一例を示す図

【図２９】認証情報生成情報格納部１００９の別の一例を示す図

【図３０】検証情報格納部１２１５の別の一例を示す図

【図３１】認証情報生成情報格納部１００９の別の一例を示す図

【図３２】検証情報格納部１２１５の別の一例を示す図

【図３３】認証情報ＡＵＴＨの別の検証方法の一例（ステップ１）を示す図

【図３４】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２）を示す図

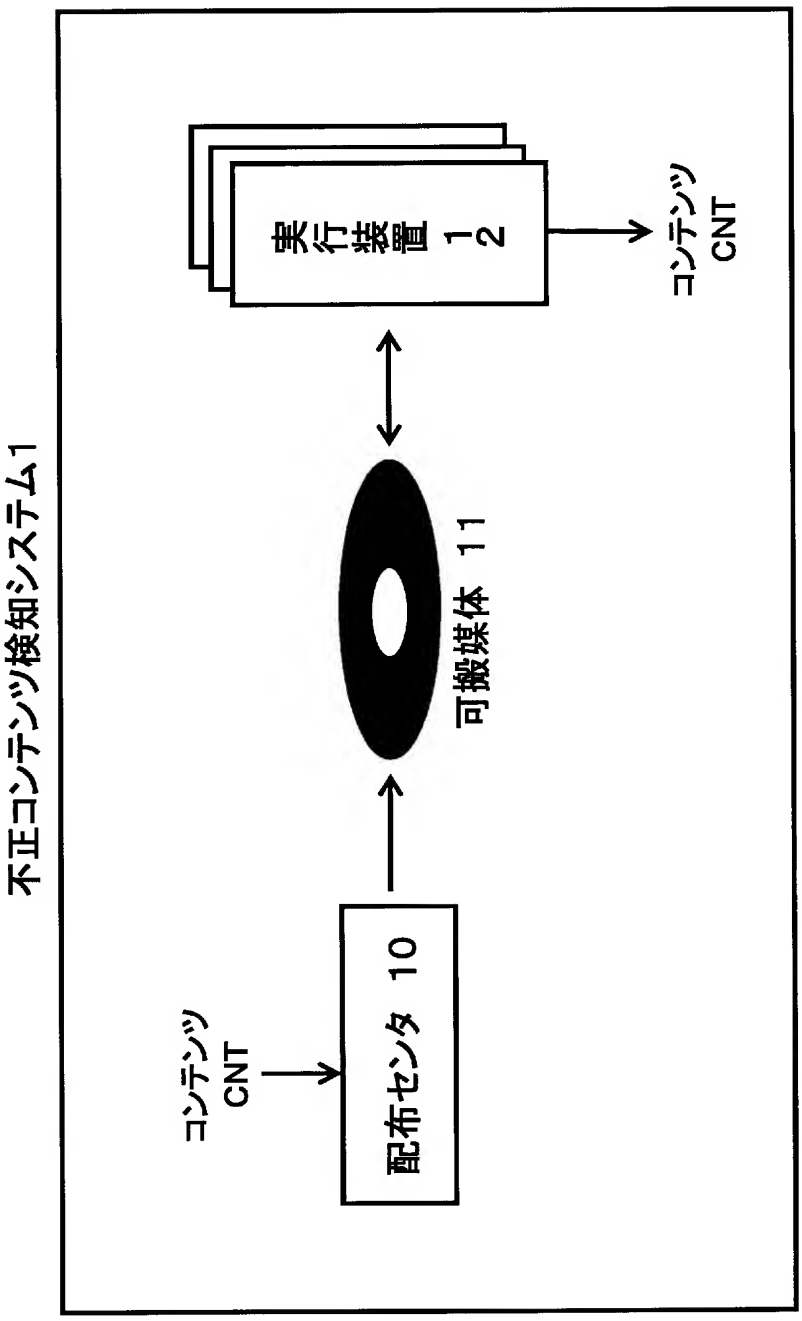
【図３５】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２の詳細１）を示す図

【図３６】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２の詳細２）を示す図

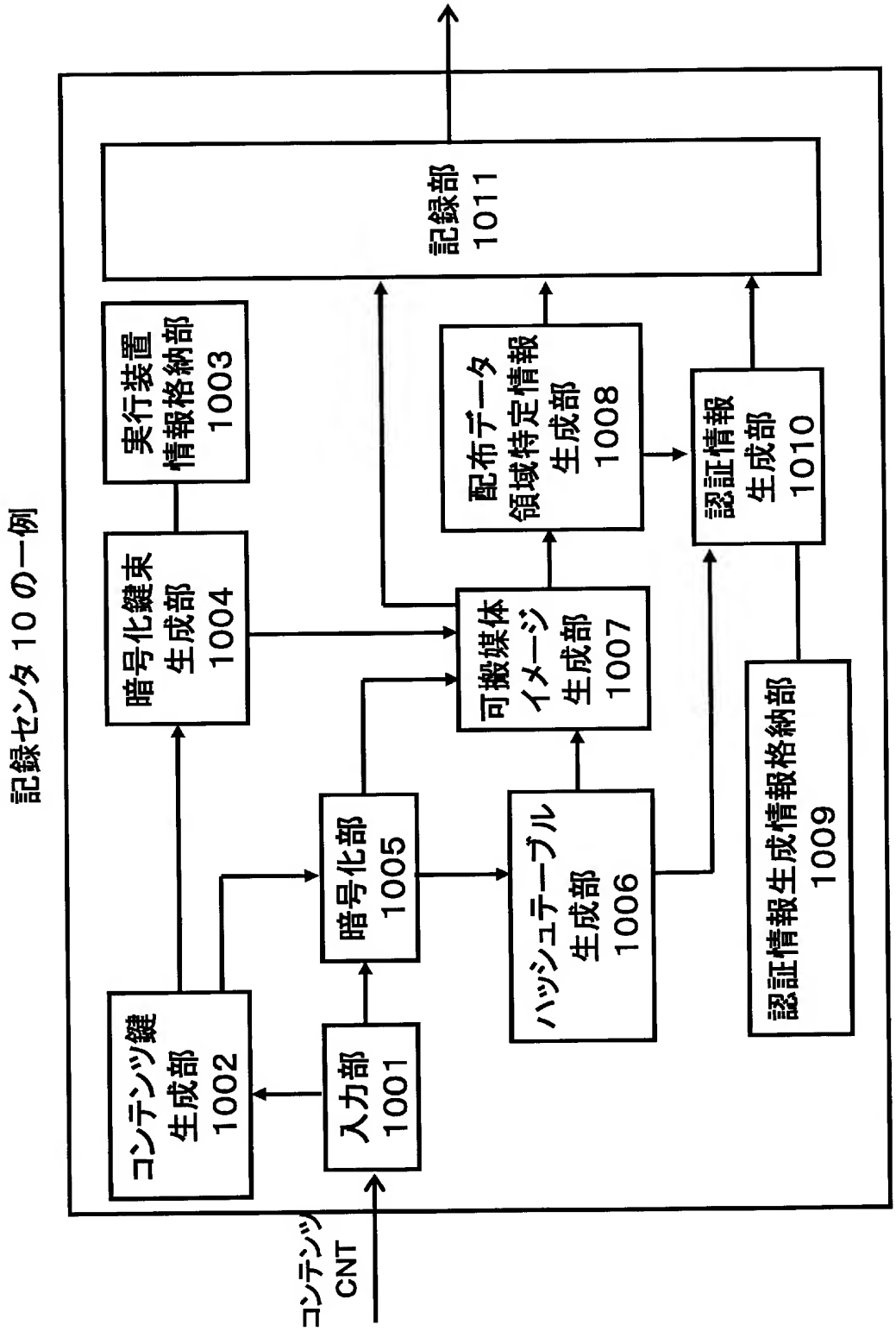
【図３７】従来技術の可搬媒体に記録されるデータの構成を示す図

【符号の説明】
【０１２５】
１０　配布センタ
１１　可搬媒体
１２　実行装置
１００１　入力部
１００２　コンテンツ鍵生成部
１００３　実行装置情報格納部
１００４　暗号化鍵束生成部
１００５　暗号化部
１００６　ハッシュテーブル生成部
１００７　可搬媒体イメージ生成部
１００８　配布データ領域特定情報生成部
１００９　認証情報生成情報格納部
１０１０　認証情報生成部
１０１１　記録部
１２０　ドライブ部
１２１　コンテンツ実行部
１２０１　取得部
１２０２　配布データ領域特定情報格納部
１２０３　第一秘密鍵格納部
１２０４　第一秘匿通信処理部
１２１１　デバイス鍵格納部
１２１２　コンテンツ鍵取得部
１２１３　第二秘密鍵格納部
１２１４　第二秘匿通信処理部
１２１５　検証情報格納部
１２１６　認証情報検証部
１２１７　実行部

【書類名】図面
【図１】



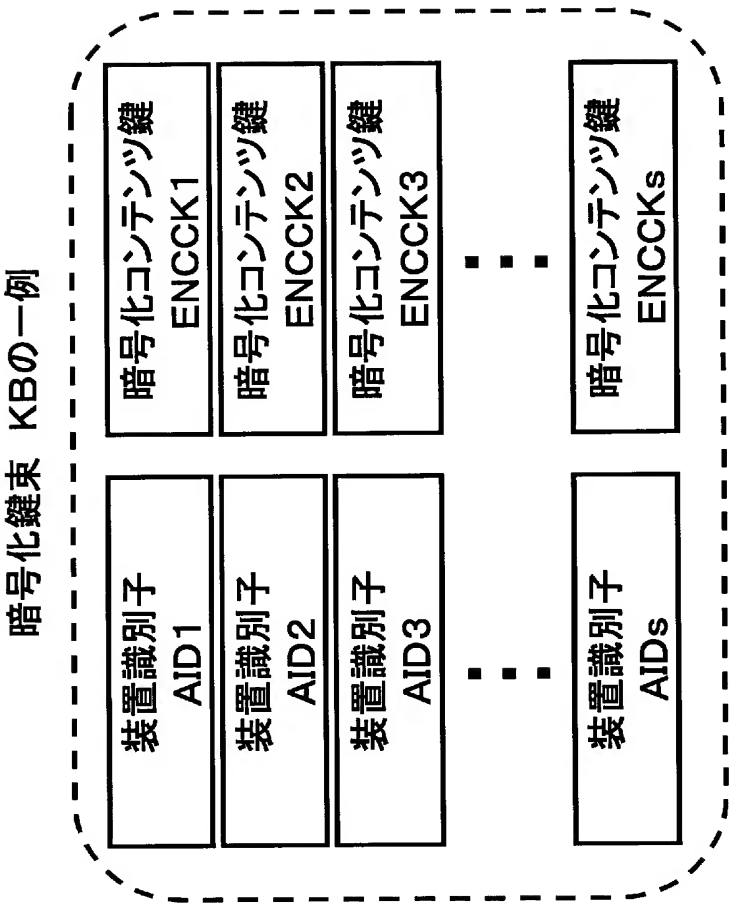
【図２】


記録センタ10の一例
コンテンツCNT
入力部 1001
コンテンツ鍵生成部 1002
暗号化部 1005
ハッシュテーブル生成部 1006
暗号化鍵束生成部 1004
実行装置情報格納部 1003
可搬媒体イメージ生成部 1007
配布データ領域特定情報生成部 1008
認証情報生成部 1009
認証情報生成部 1010
記録部 1011

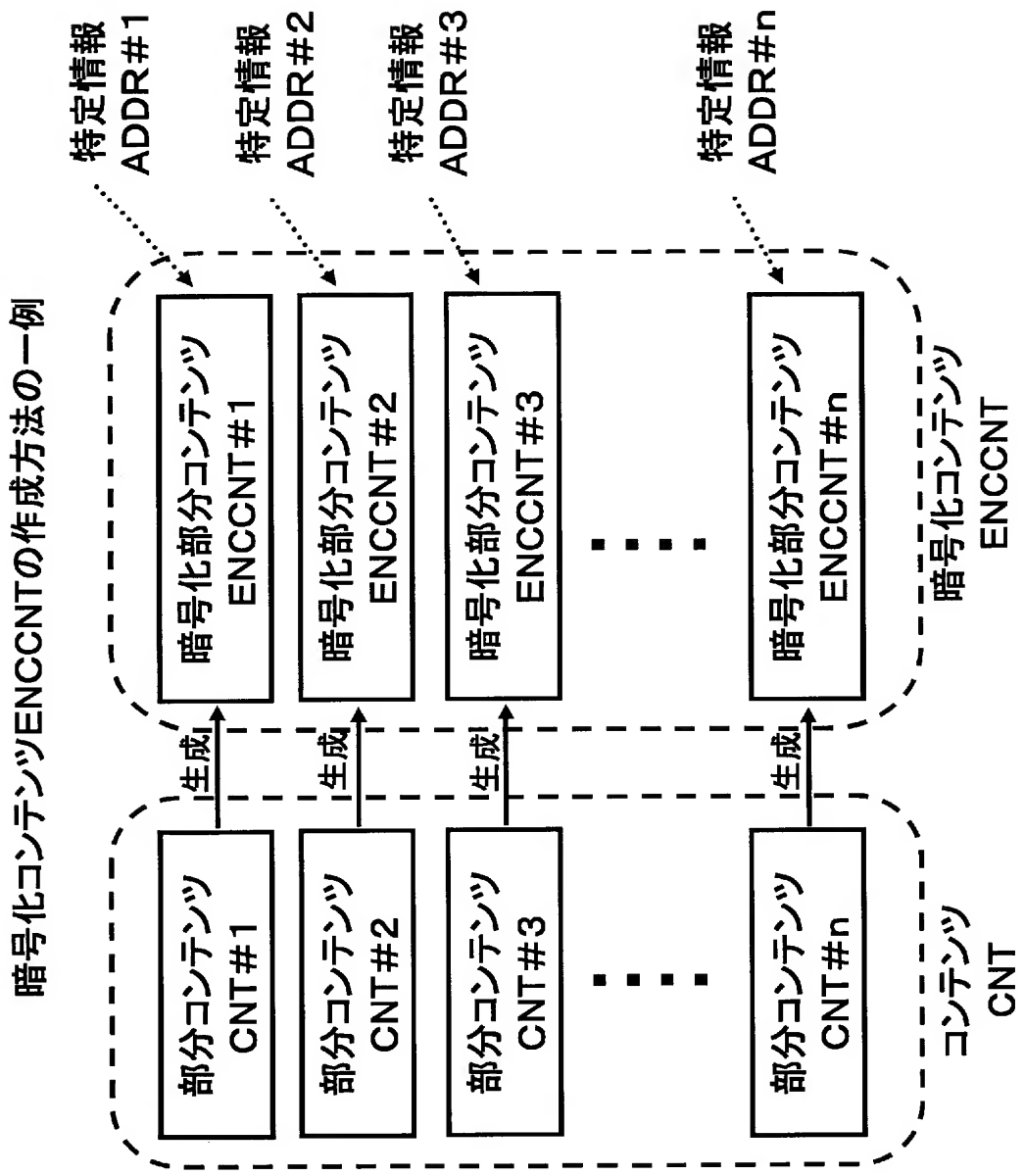
【図３】

実行装置情報格納部1003の一例

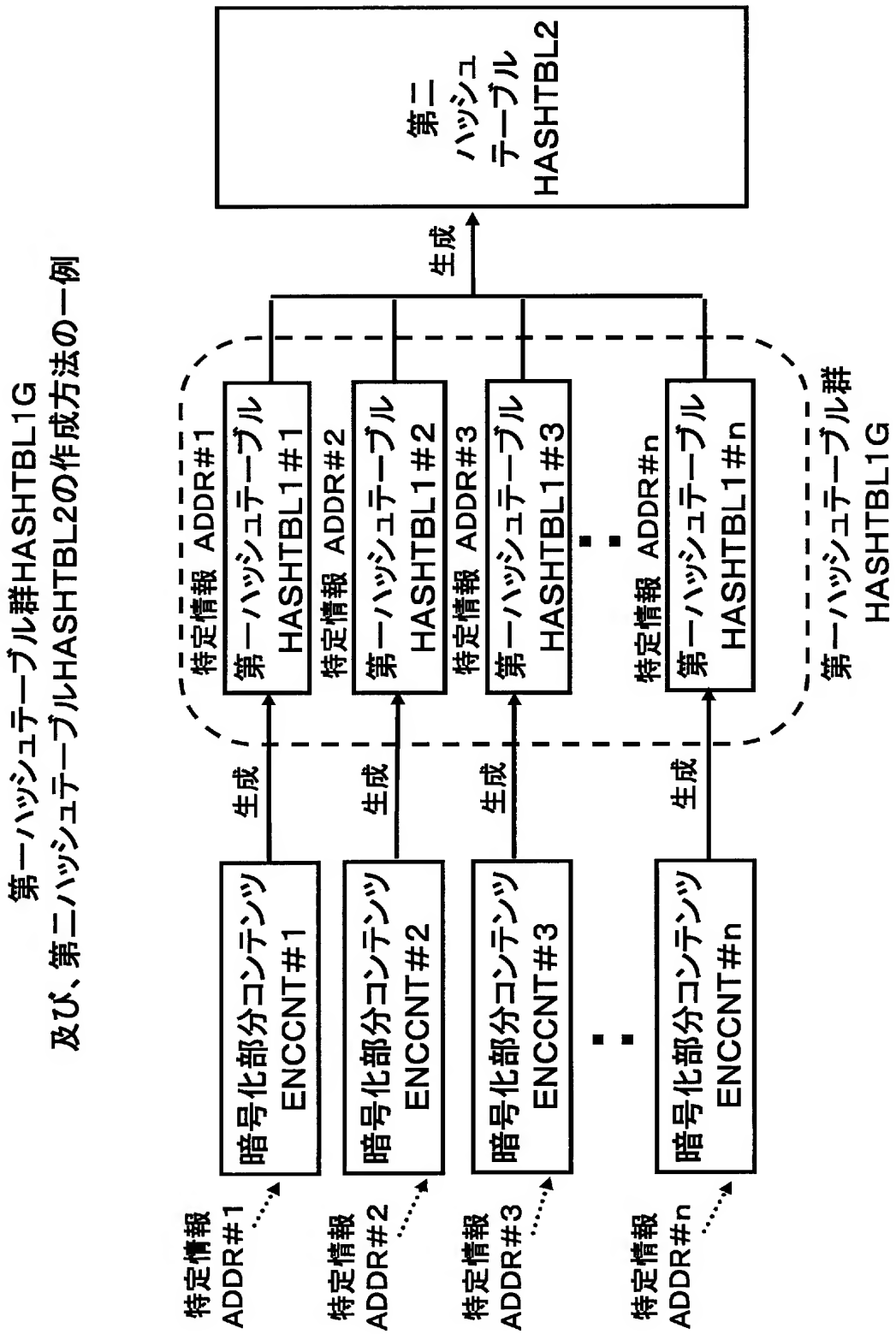
【図４】


暗号化鍵束　KBの一例
装置識別子
AID1
装置識別子
AID2
装置識別子
AID3
装置識別子
AIDs
暗号化コンテンツ鍵
ENCCK1
暗号化コンテンツ鍵
ENCCK2
暗号化コンテンツ鍵
ENCCK3
暗号化コンテンツ鍵
ENCCKs

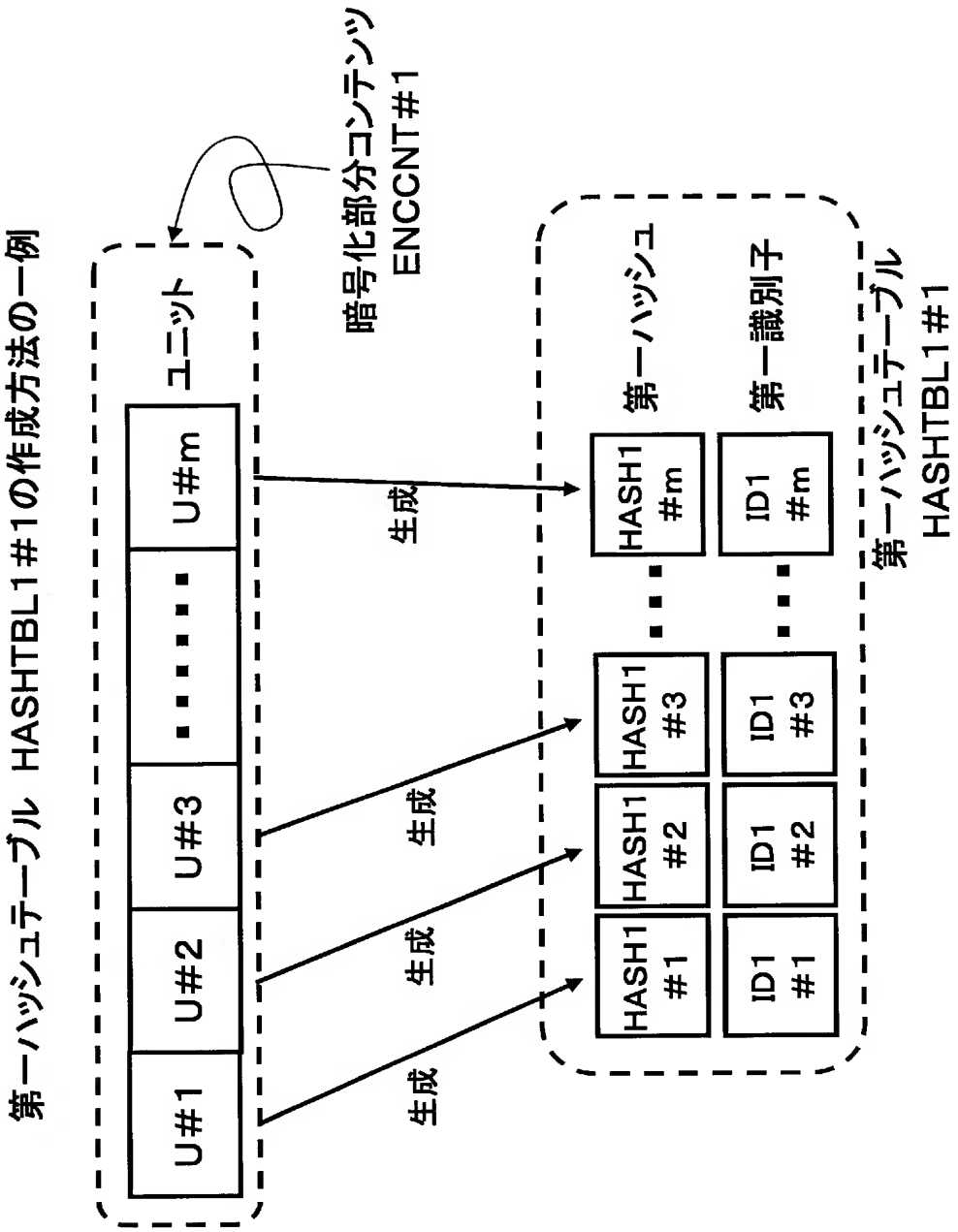
【図５】


暗号化コンテンツENCCNTの作成方法の一例
特定情報 ADDR#1
特定情報 ADDR#2
特定情報 ADDR#3
特定情報 ADDR#n
暗号化部分コンテンツ ENCCNT#1
暗号化部分コンテンツ ENCCNT#2
暗号化部分コンテンツ ENCCNT#3
暗号化部分コンテンツ ENCCNT#n
暗号化コンテンツ ENCCNT
生成
生成
生成
生成
部分コンテンツ CNT#1
部分コンテンツ CNT#2
部分コンテンツ CNT#3
部分コンテンツ CNT#n
コンテンツ CNT

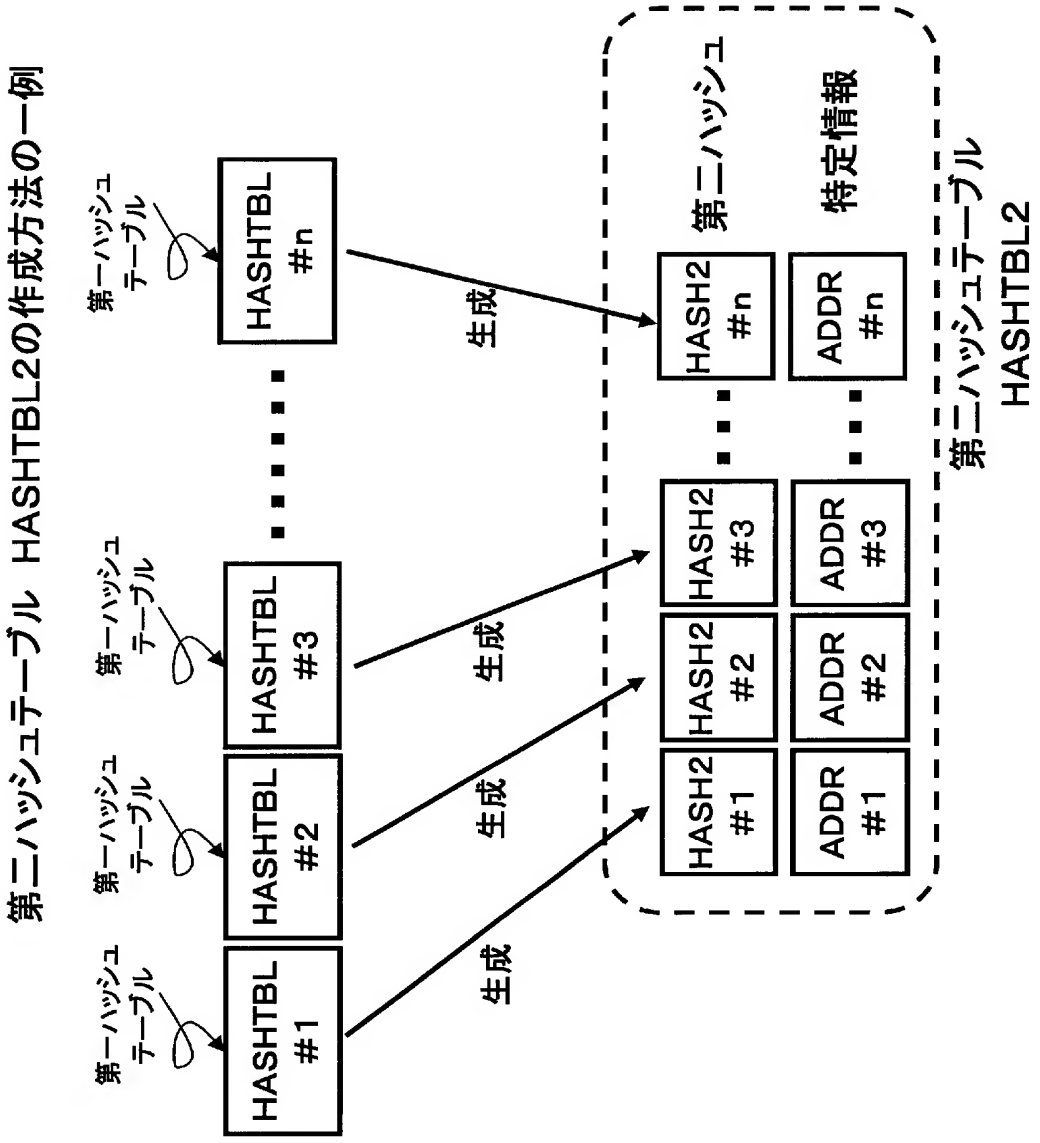
【図６】


第一ハッシュテーブル群HASHTBL1G
及び、第二ハッシュテーブルHASHTBL2の作成方法の一例
第二
ハッシュ
テーブル
HASHTBL2
生成
特定情報 ADDR#1
第一ハッシュテーブル
HASHTBL1#1
特定情報 ADDR#2
第一ハッシュテーブル
HASHTBL1#2
特定情報 ADDR#3
第一ハッシュテーブル
HASHTBL1#3
特定情報 ADDR#n
第一ハッシュテーブル
HASHTBL1#n
第一ハッシュテーブル群
HASHTBL1G
生成
生成
生成
生成
暗号化部分コンテンツ
ENCCNT#1
暗号化部分コンテンツ
ENCCNT#2
暗号化部分コンテンツ
ENCCNT#3
暗号化部分コンテンツ
ENCCNT#n
特定情報
ADDR#1
特定情報
ADDR#2
特定情報
ADDR#3
特定情報
ADDR#n

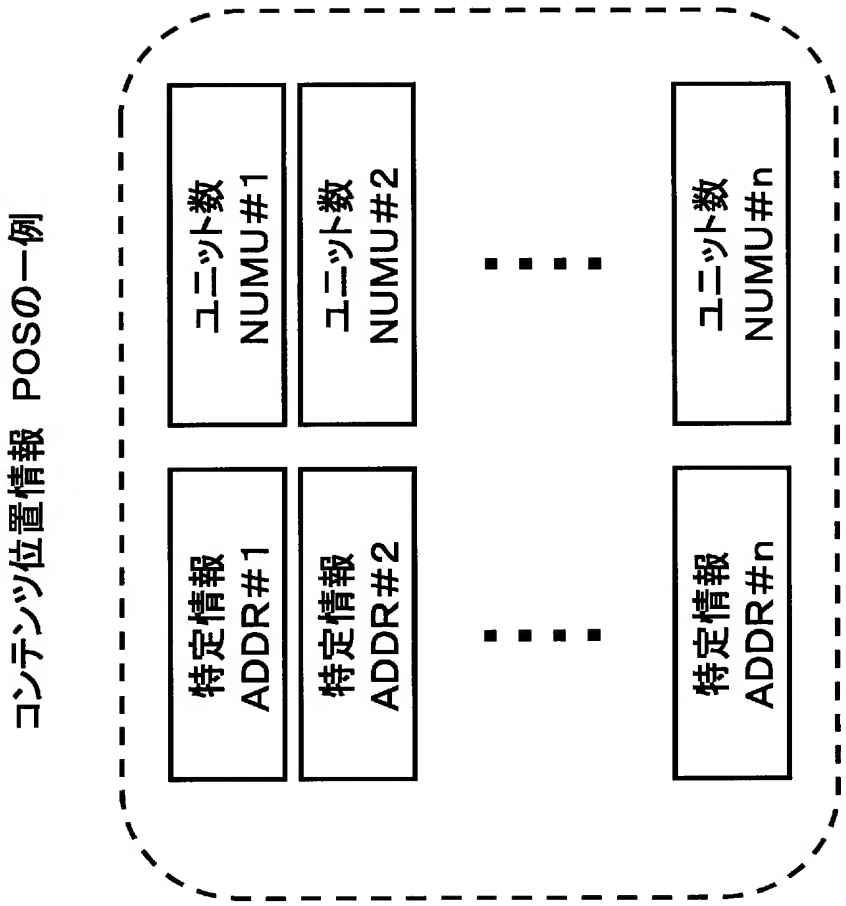
【図７】


第一ハッシュテーブル HASHTBL1＃1の作成方法の一例
ユニット
U#1
U#2
U#3
U#m
暗号化部分コンテンツ
ENCCNT＃1
生成
生成
生成
生成
第一ハッシュ
第一識別子
HASH1 #1
HASH1 #2
HASH1 #3
HASH1 #m
ID1 #1
ID1 #2
ID1 #3
ID1 #m
第一ハッシュテーブル
HASHTBL1＃1

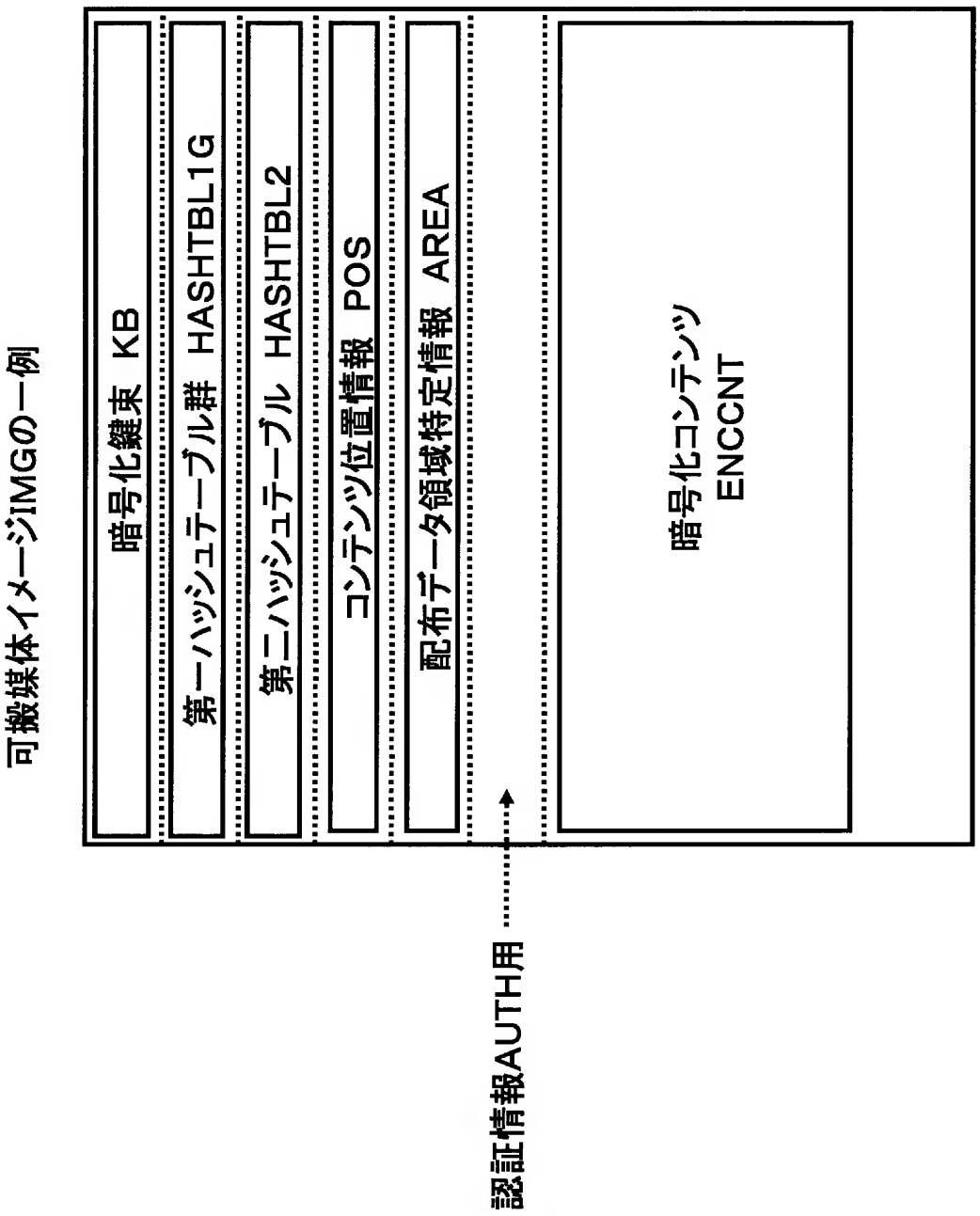
【図８】


第二ハッシュテーブル HASHTBL2の作成方法の一例
第一ハッシュテーブル
HASHTBL #1
HASHTBL #2
HASHTBL #3
HASHTBL #n
生成
第二ハッシュテーブル HASHTBL2
第二ハッシュ
特定情報
HASH2 #1
HASH2 #2
HASH2 #3
HASH2 #n
ADDR #1
ADDR #2
ADDR #3
ADDR #n

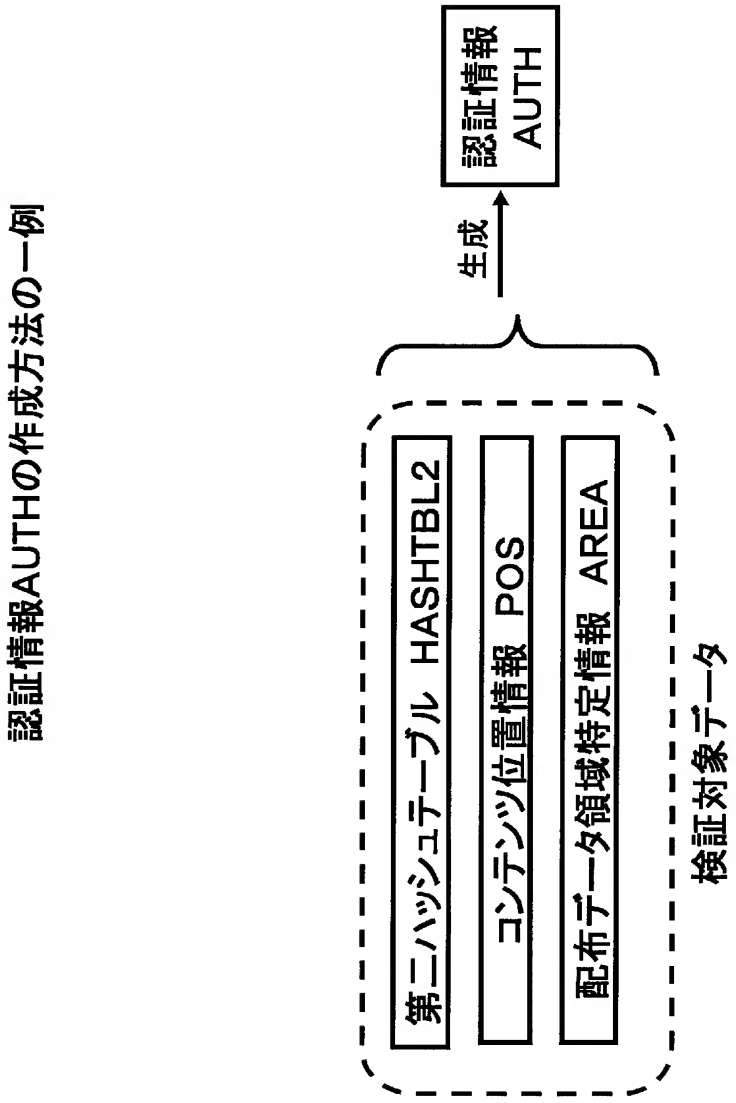
【図９】


コンテンツ位置情報　POSの一例
特定情報
ADDR#1
特定情報
ADDR#2
特定情報
ADDR#n
ユニット数
NUMU#1
ユニット数
NUMU#2
ユニット数
NUMU#n

【図１０】

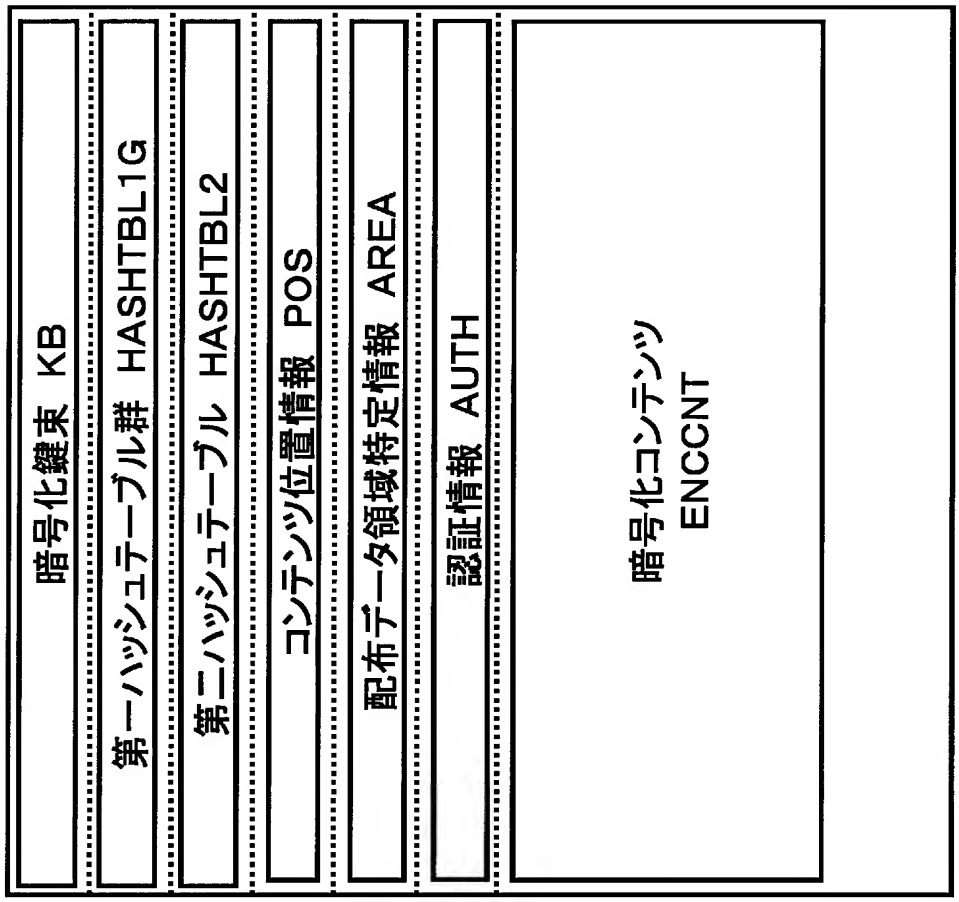

可搬媒体イメージIMGの一例
暗号化鍵束 KB
第一ハッシュテーブル群 HASHTBL1G
第二ハッシュテーブル HASHTBL2
コンテンツ位置情報 POS
配布データ領域特定情報 AREA
暗号化コンテンツ
ENCCNT
認証情報AUTH用

【図１１】

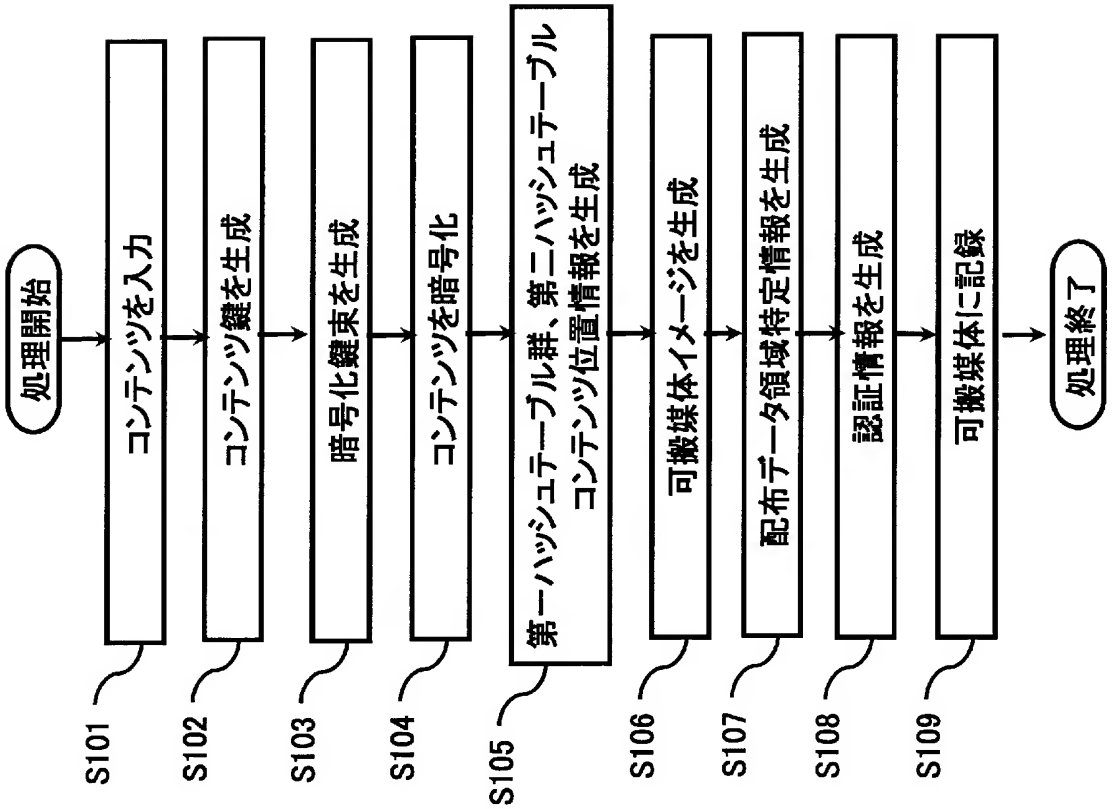

認証情報AUTHの作成方法の一例
認証情報
AUTH
生成
第二ハッシュテーブル HASHTBL2
コンテンツ位置情報 POS
配布データ領域特定情報 AREA
検証対象データ

【図１２】

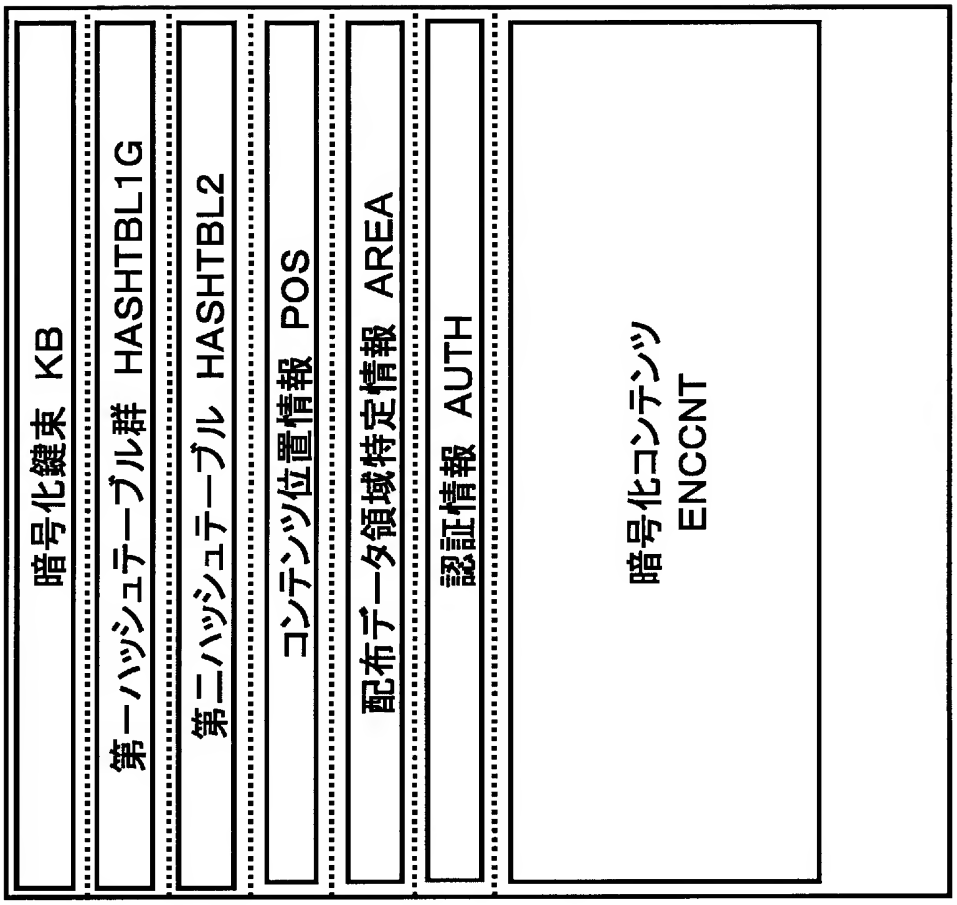
第二可搬媒体イメージIMG2の一例



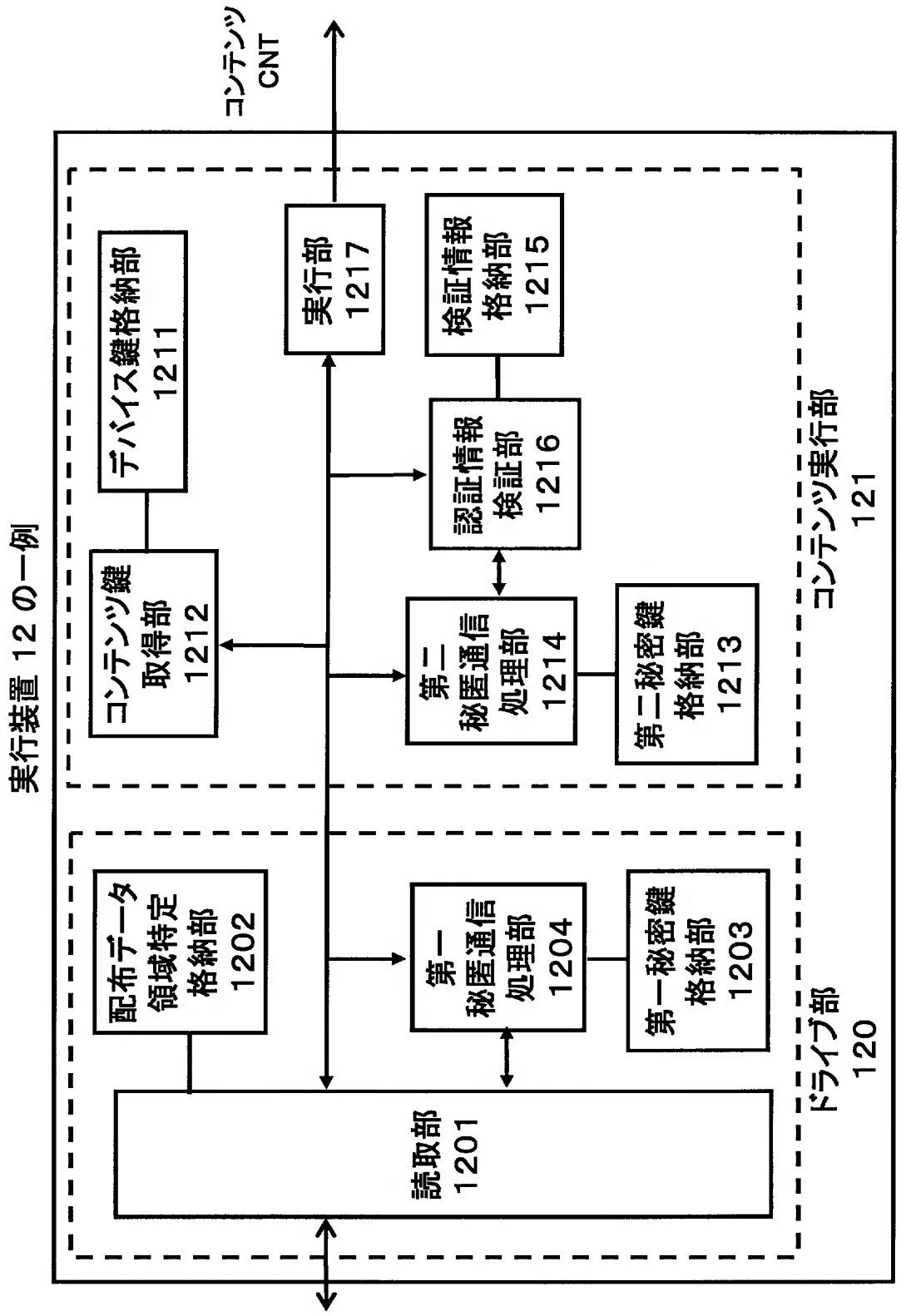
【図１３】


処理開始
コンテンツを入力
コンテンツ鍵を生成
暗号化鍵束を生成
コンテンツを暗号化
第一ハッシュテーブル群、第二ハッシュテーブル
コンテンツ位置情報を生成
可搬媒体イメージを生成
配布データ領域特定情報を生成
認証情報を生成
可搬媒体に記録
処理終了
S101
S102
S103
S104
S105
S106
S107
S108
S109

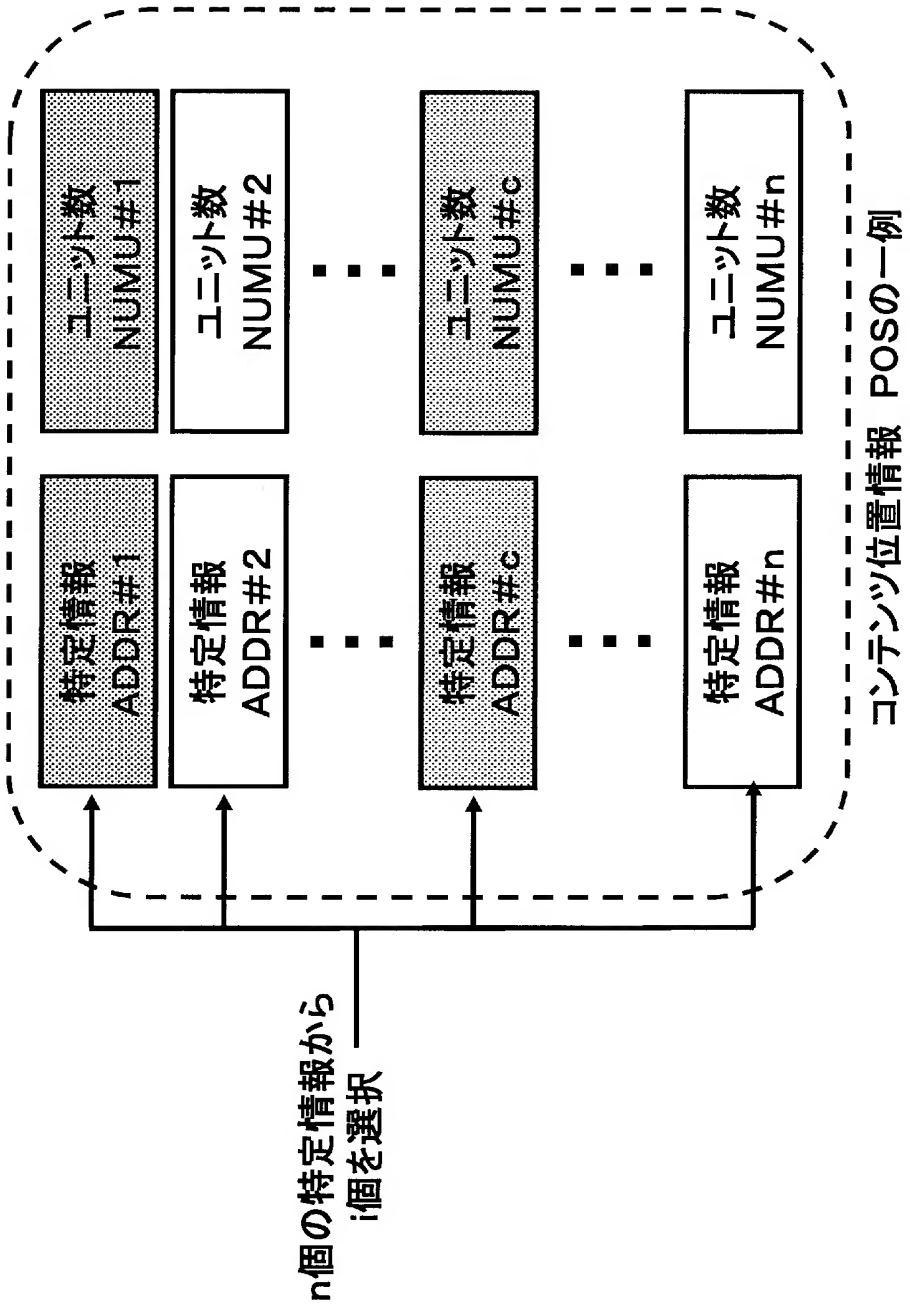
【図１４】


可搬媒体11に記録されるデータの一例
暗号化鍵束 KB
第一ハッシュテーブル群 HASHTBL1G
第二ハッシュテーブル HASHTBL2
コンテンツ位置情報 POS
配布データ領域特定情報 AREA
認証情報 AUTH
暗号化コンテンツ
ENCCNT

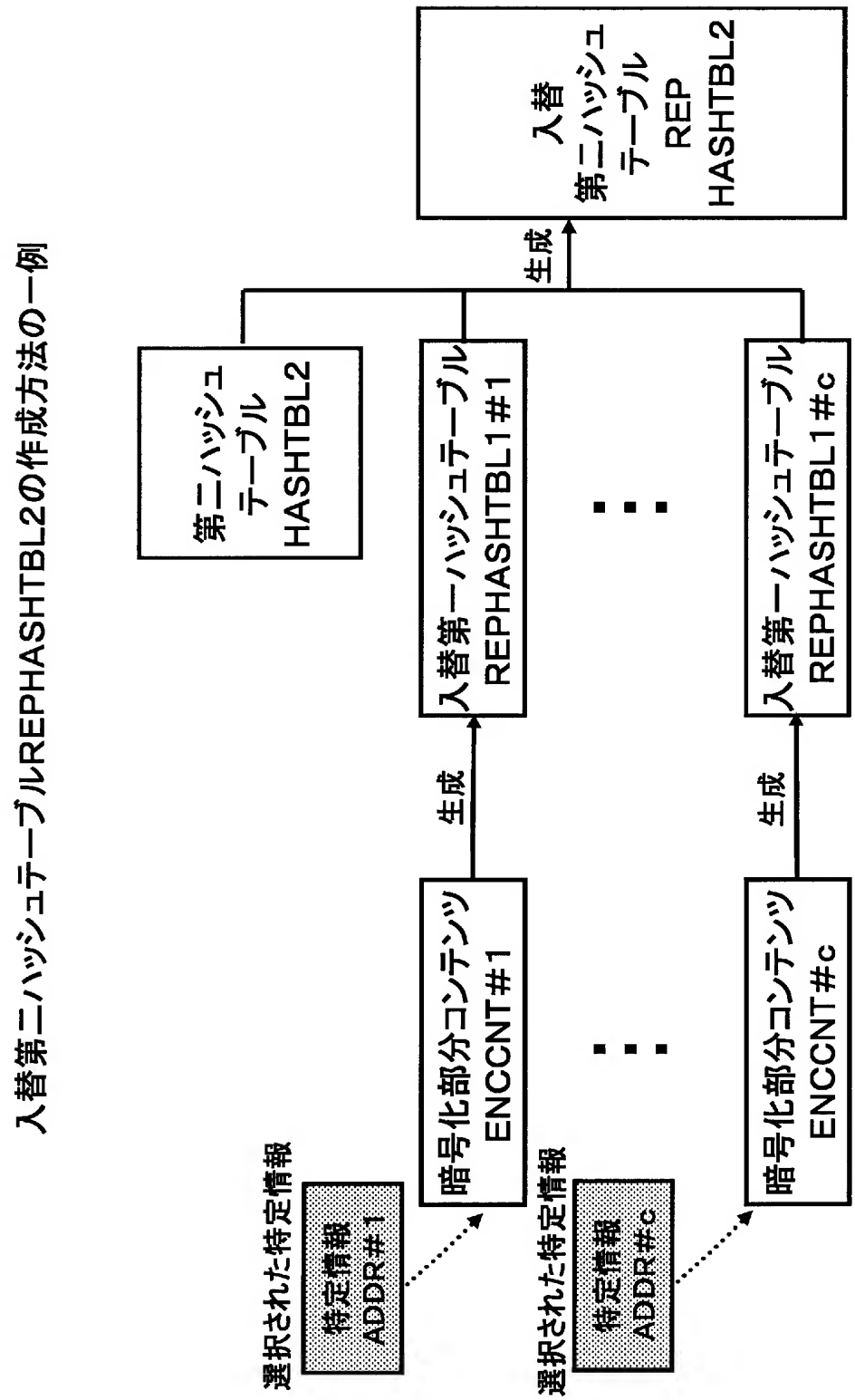
【図１５】


実行装置 12 の一例
コンテンツ
CNT
実行部
1217
検証情報
格納部
1215
デバイス鍵格納部
1211
認証情報
検証部
1216
コンテンツ鍵
取得部
1212
第二
秘匿通信
処理部
1214
第二秘密鍵
格納部
1213
コンテンツ実行部
121
配布データ
領域特定
格納部
1202
第一
秘匿通信
処理部
1204
第一秘密鍵
格納部
1203
読取部
1201
ドライブ部
120

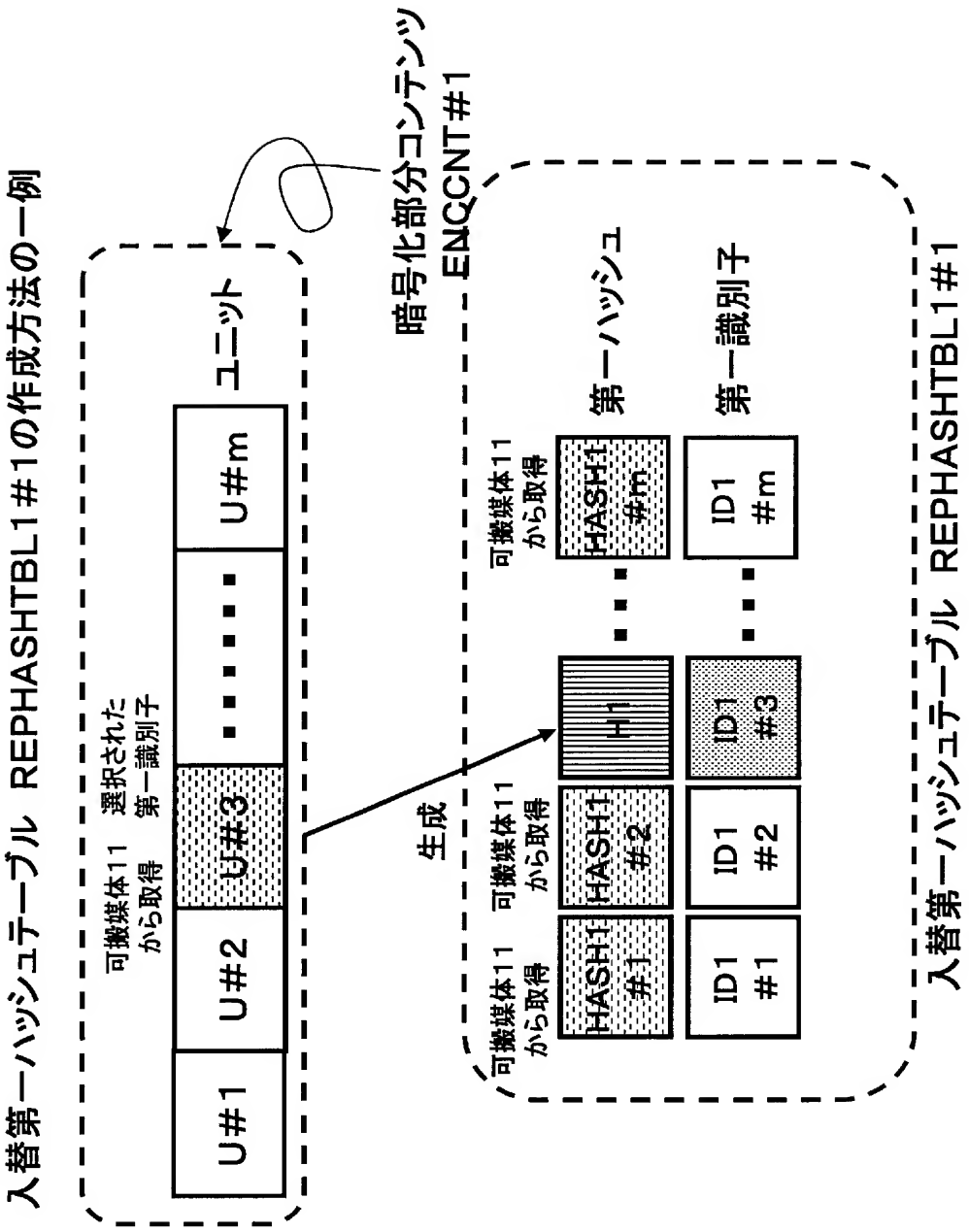
【図１６】


ユニット数
NUMU#1
ユニット数
NUMU#2
ユニット数
NUMU#c
ユニット数
NUMU#n
特定情報
ADDR#1
特定情報
ADDR#2
特定情報
ADDR#c
特定情報
ADDR#n
コンテンツ位置情報　POSの一例
n個の特定情報から
i個を選択

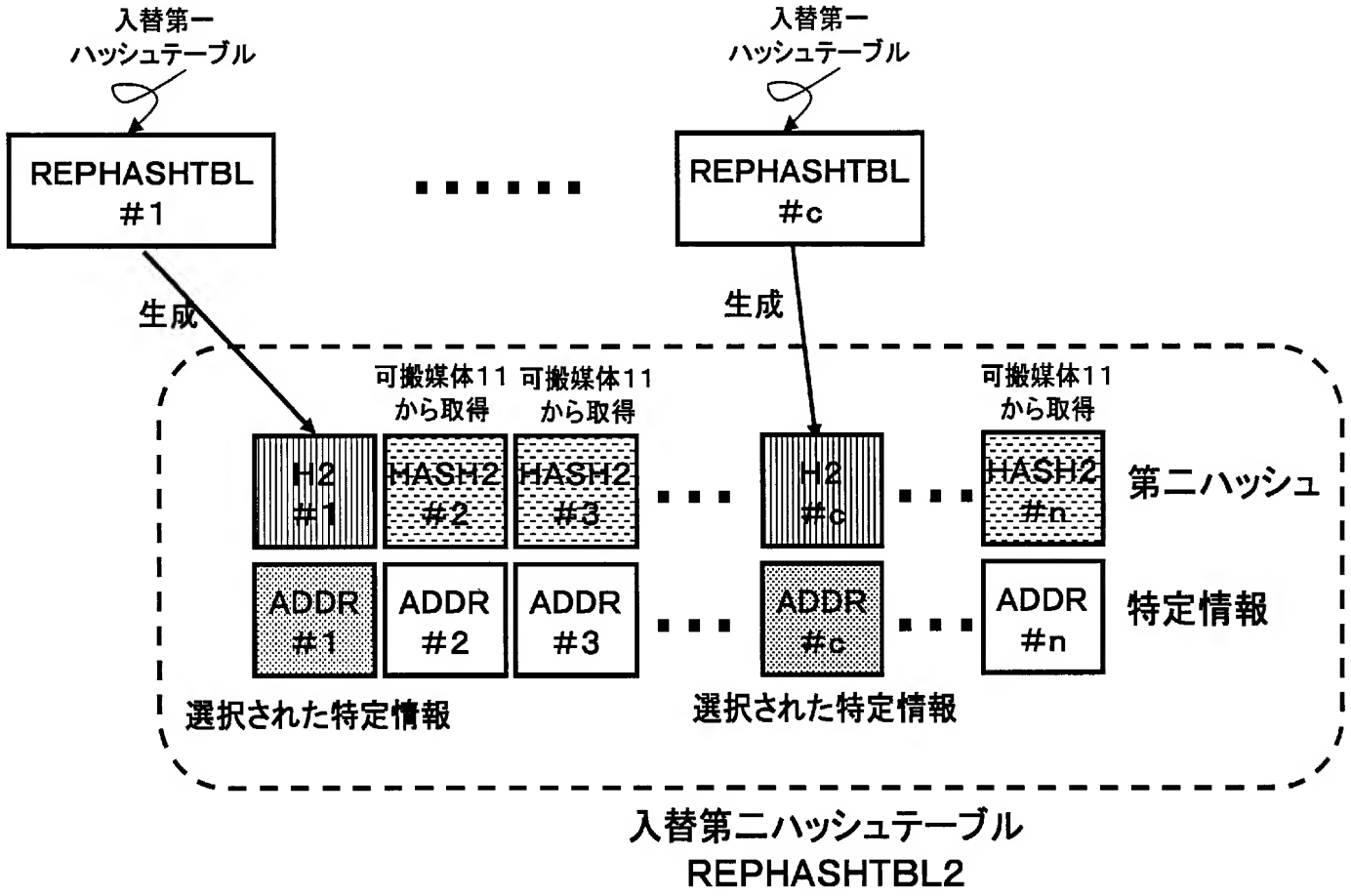
【図１７】


入替第ニハッシュテーブルREPHASHTBL2の作成方法の一例
入替
第ニハッシュ
テーブル
REP
HASHTBL2
生成
第ニハッシュ
テーブル
HASHTBL2
入替第一ハッシュテーブル
REPHASHTBL1＃1
入替第一ハッシュテーブル
REPHASHTBL1＃c
生成
生成
暗号化部分コンテンツ
ENCCNT＃1
暗号化部分コンテンツ
ENCCNT＃c
選択された特定情報
特定情報
ADDR＃1
選択された特定情報
特定情報
ADDR＃c

【図１８】

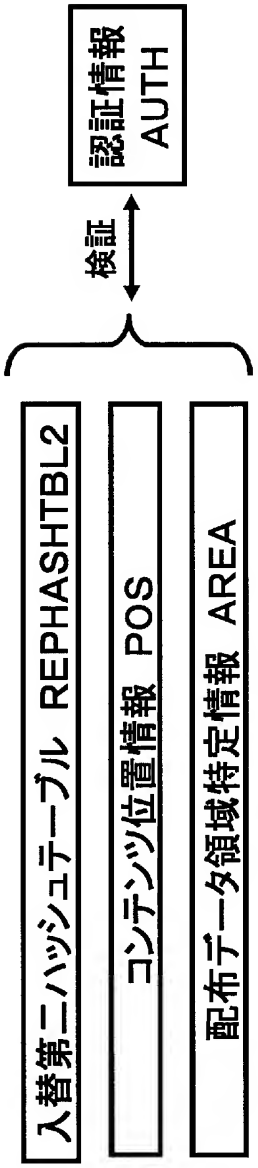

入替第一ハッシュテーブル REPHASHTBL1#1の作成方法の一例
ユニット
U#1
U#2
U#3
U#m
可搬媒体11 選択された 第一識別子 から取得
暗号化部分コンテンツ ENCCNT#1
生成
可搬媒体11 から取得
H1
可搬媒体11 から取得
HASH1 #1
HASH1 #2
HASH1 #m
第一ハッシュ
ID1 #1
ID1 #2
ID1 #3
ID1 #m
第一識別子
入替第一ハッシュテーブル REPHASHTBL1#1

入替第二ハッシュテーブル　REPHASHTBL2の作成方法の一例

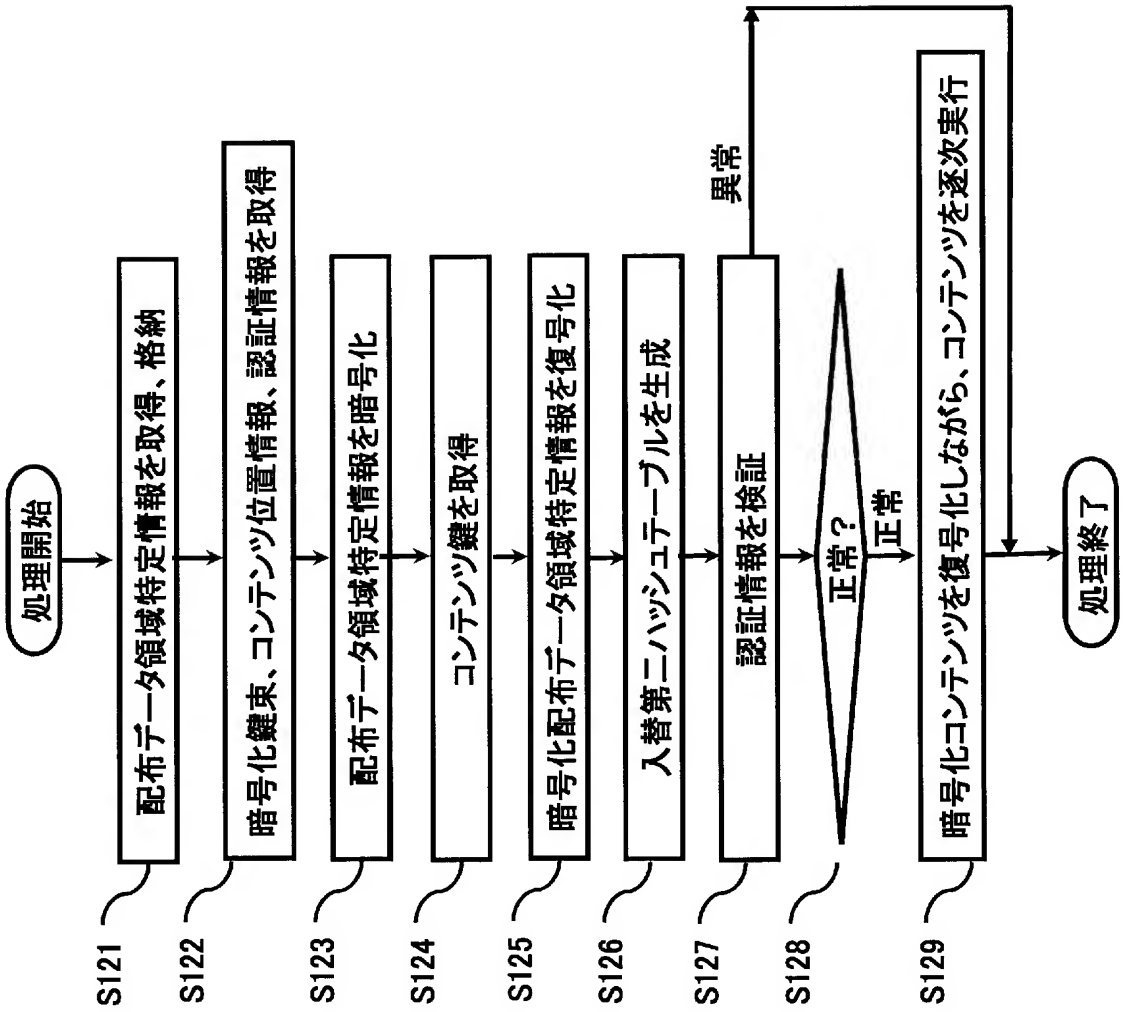


【図２０】

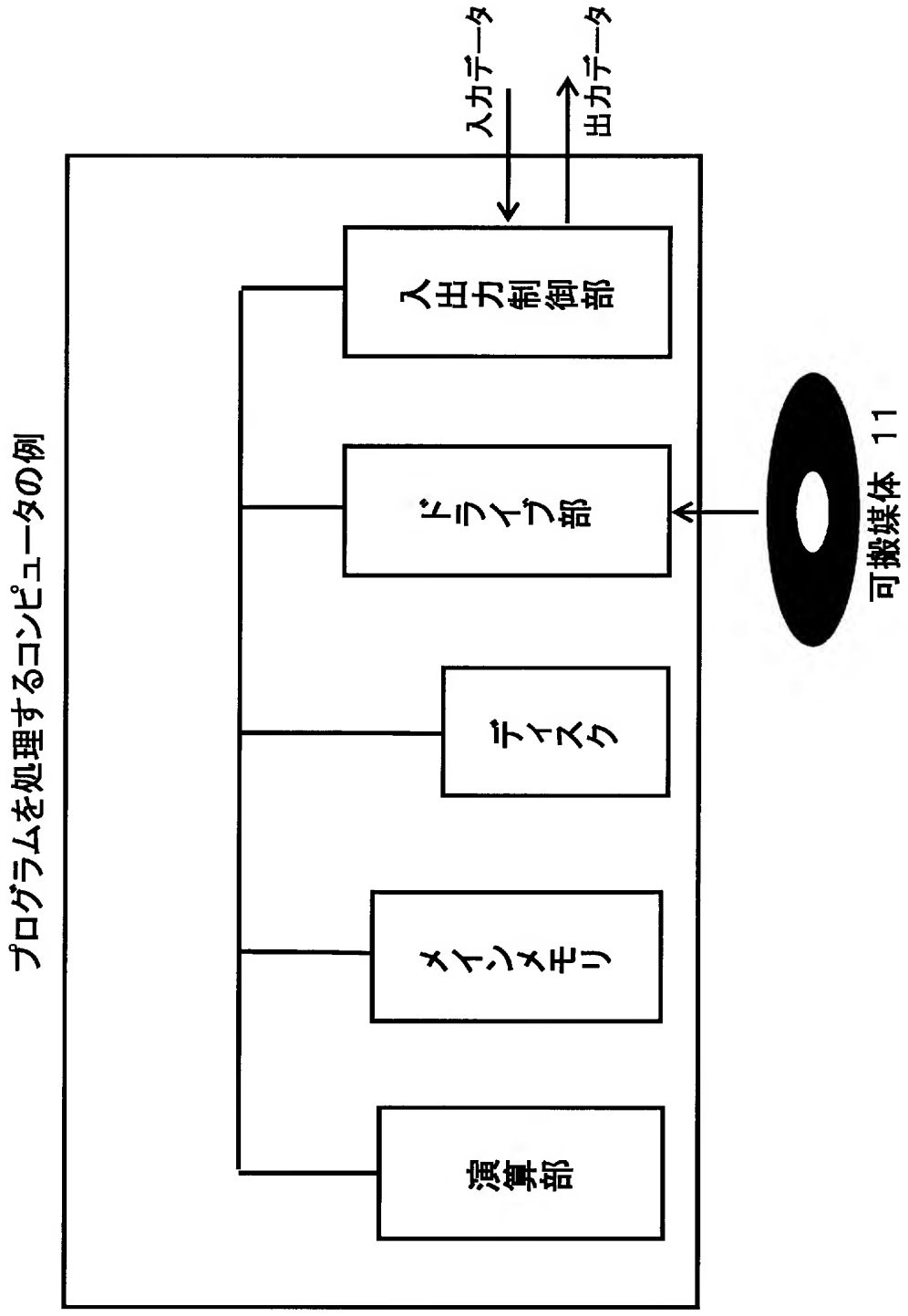
認証情報AUTHの検証方法の一例



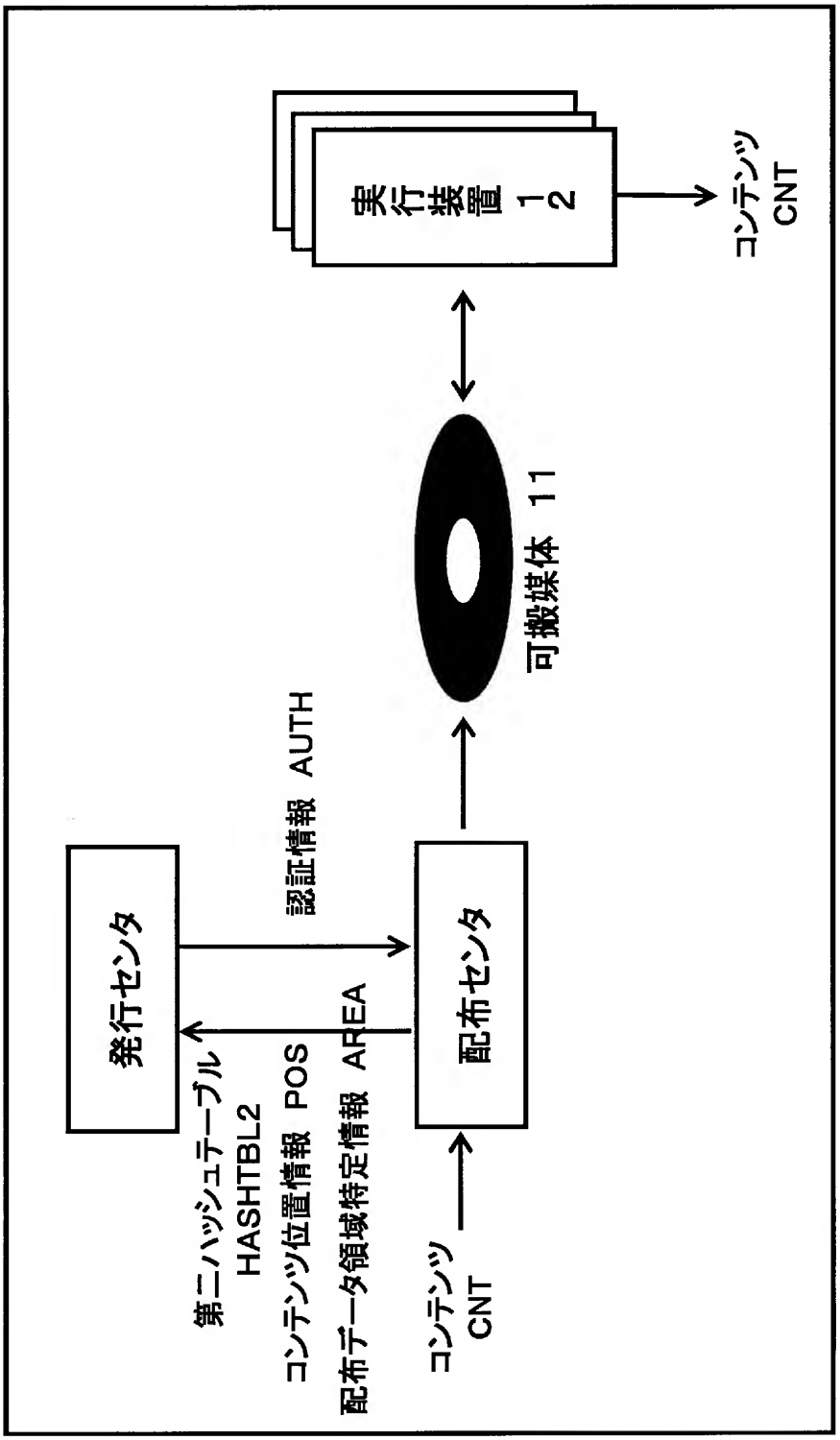
【図２１】


処理開始
配布データ領域特定情報を取得、格納
暗号化鍵束、コンテンツ位置情報、認証情報を取得
配布データ領域特定情報を暗号化
コンテンツ鍵を取得
暗号化配布データ領域特定情報を復号化
入替第二ハッシュテーブルを生成
認証情報を検証
正常？
異常
正常
暗号化コンテンツを復号化しながら、コンテンツを逐次実行
処理終了
S121
S122
S123
S124
S125
S126
S127
S128
S129

【図２２】

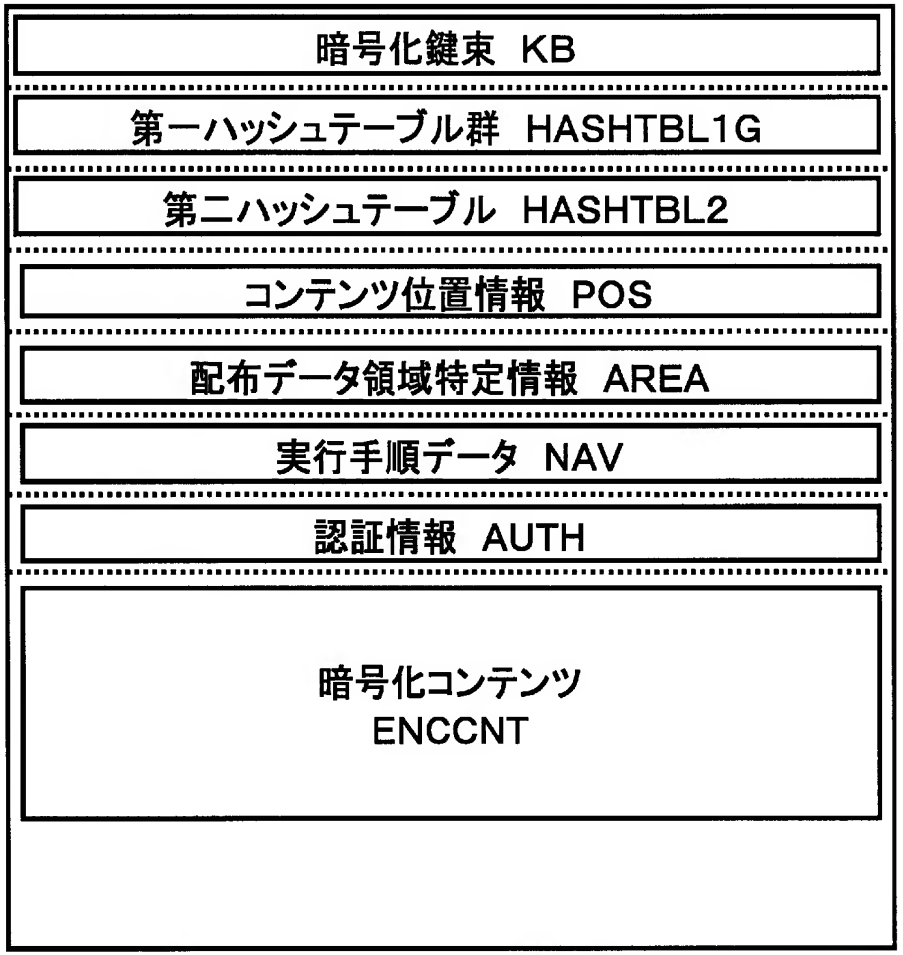

プログラムを処理するコンピュータの例
入出力制御部
ドライブ部
ディスク
メインメモリ
演算部
入力データ
出力データ
可搬媒体 11

【図２３】

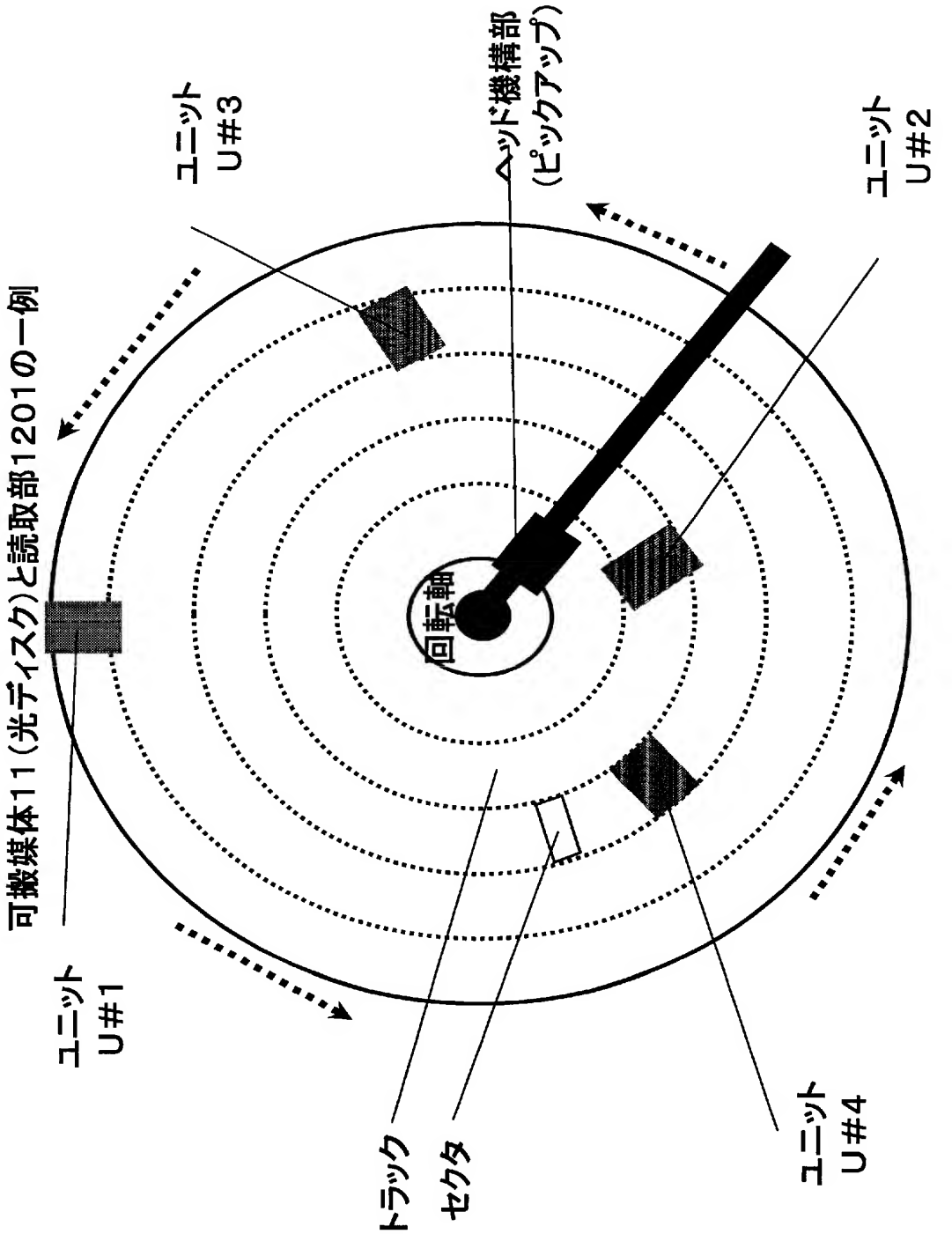

発行センタ
配布センタ
認証情報 AUTH
第二ハッシュテーブル
HASHTBL2
コンテンツ位置情報 POS
配布データ領域特定情報 AREA
コンテンツ
CNT
可搬媒体 11
実行装置 1-2
コンテンツ
CNT

【図２４】

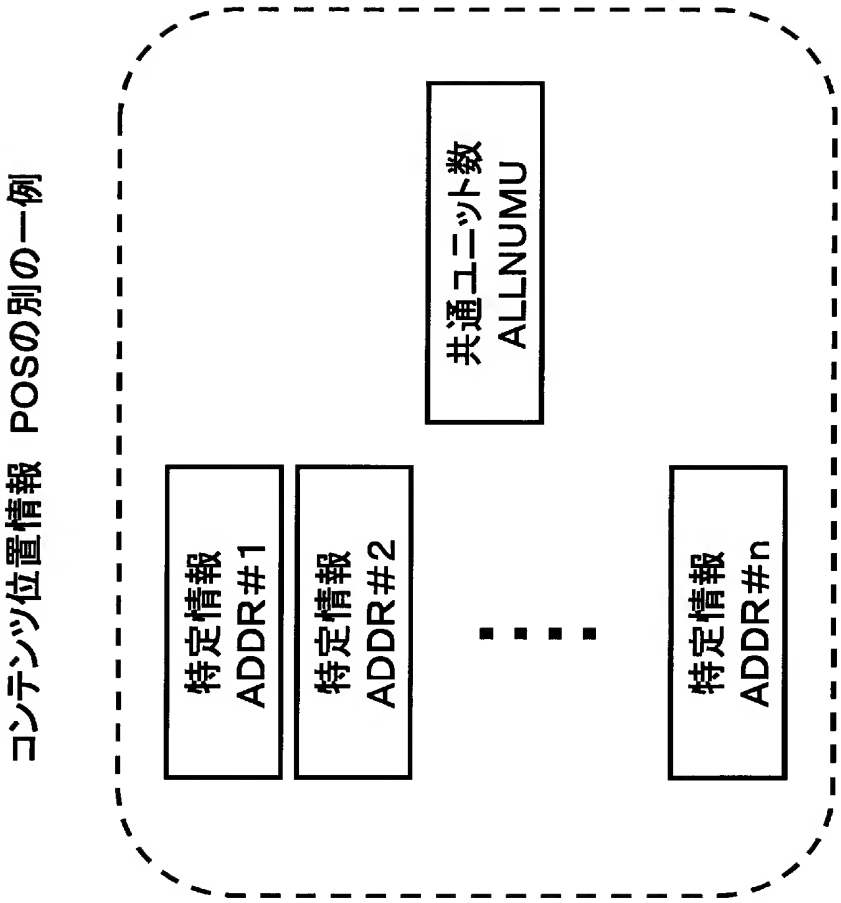
可搬媒体１１に記録されるデータの別の一例



【図２５】

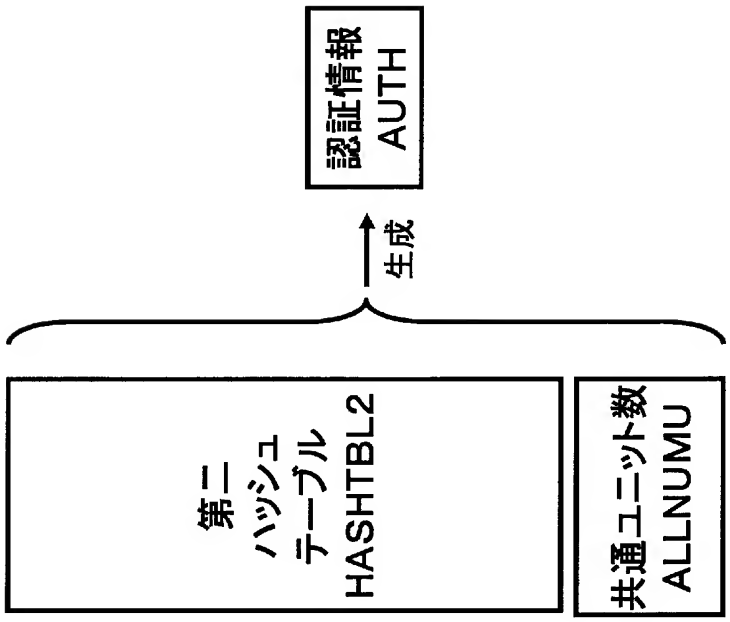

可搬媒体11(光ディスク)と読取部1201の一例
ユニット
U#1
ユニット
U#3
ヘッド機構部
(ピックアップ)
ユニット
U#2
回転軸
トラック
セクタ
ユニット
U#4

【図２６】


コンテンツ位置情報　POSの別の一例
特定情報
ADDR#1
特定情報
ADDR#2
共通ユニット数
ALLNUMU
特定情報
ADDR#n

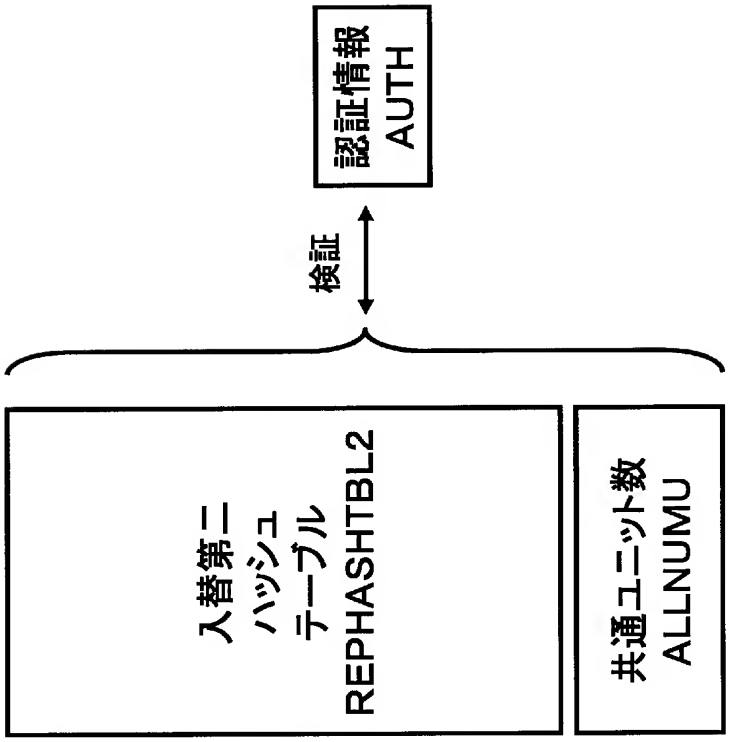
【図２７】

認証情報AUTHの作成方法の別の一例

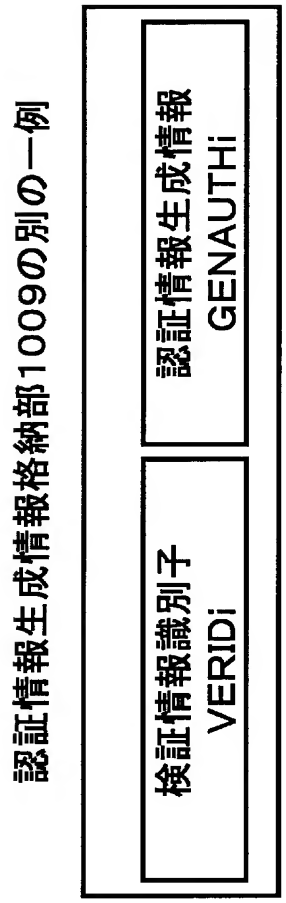


【図２８】

認証情報AUTHの検証方法の別の一例

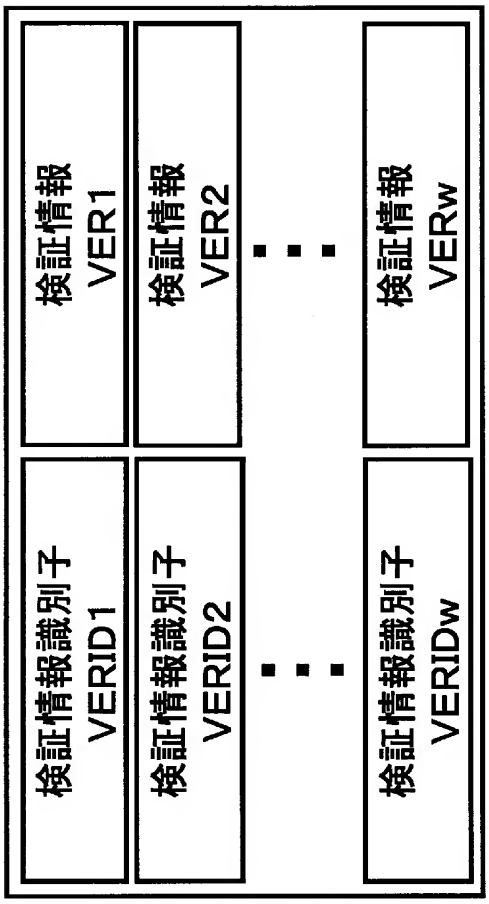


【図２９】

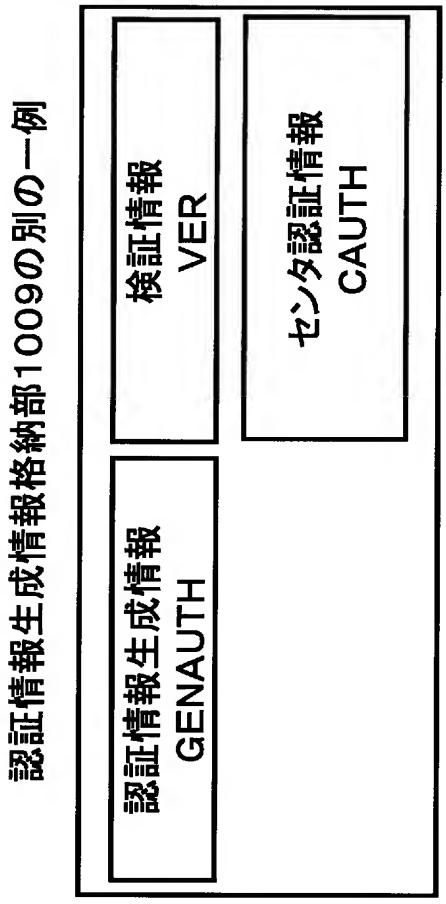


【図３０】

検証情報格納部1215の別の一例

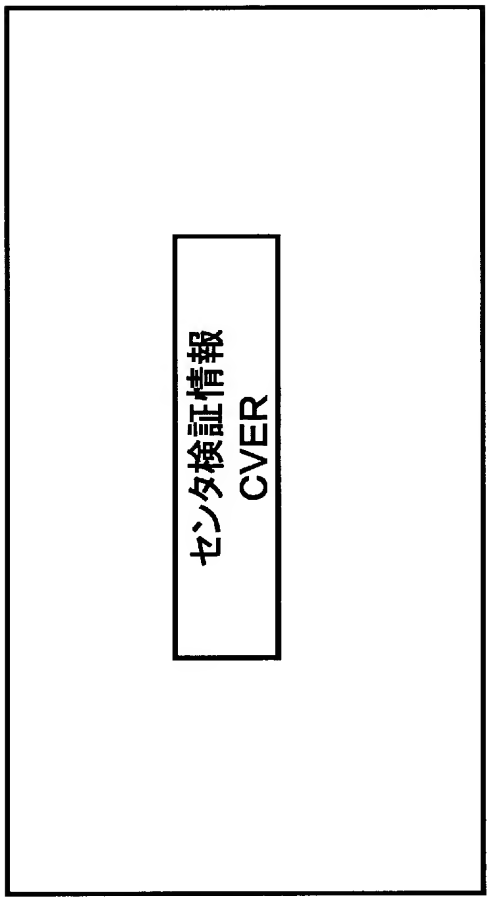


【図３１】


認証情報生成情報格納部1009の別の一例
認証情報生成情報
GENAUTH
検証情報
VER
センタ認証情報
CAUTH

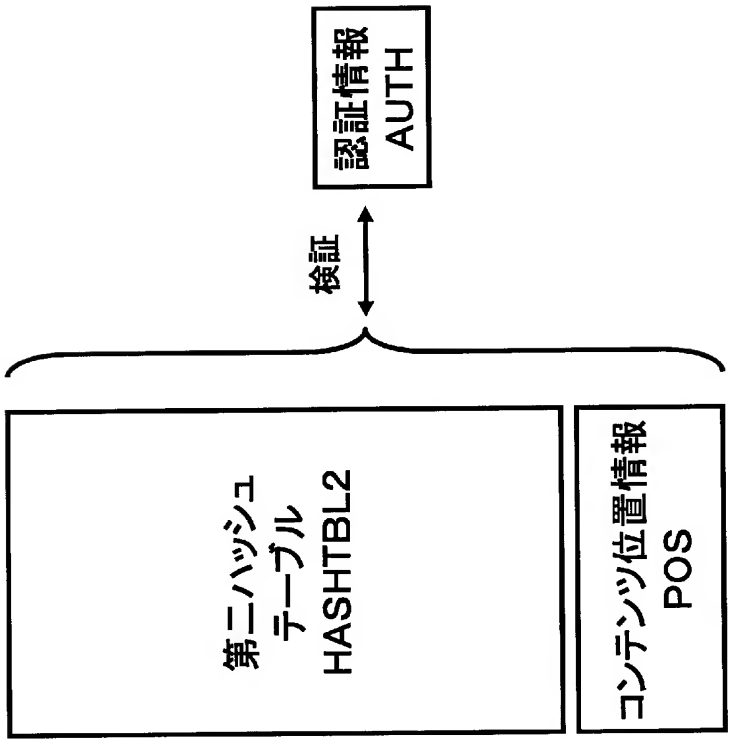
【図３２】

検証情報格納部1215の別の一例

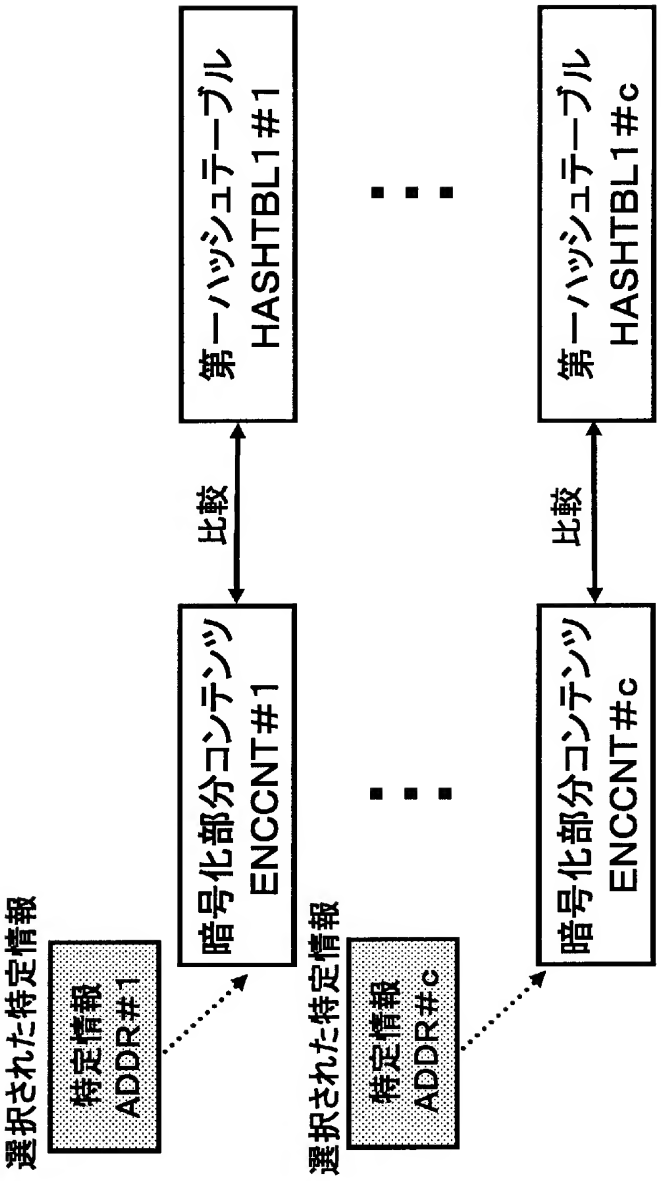


【図３３】

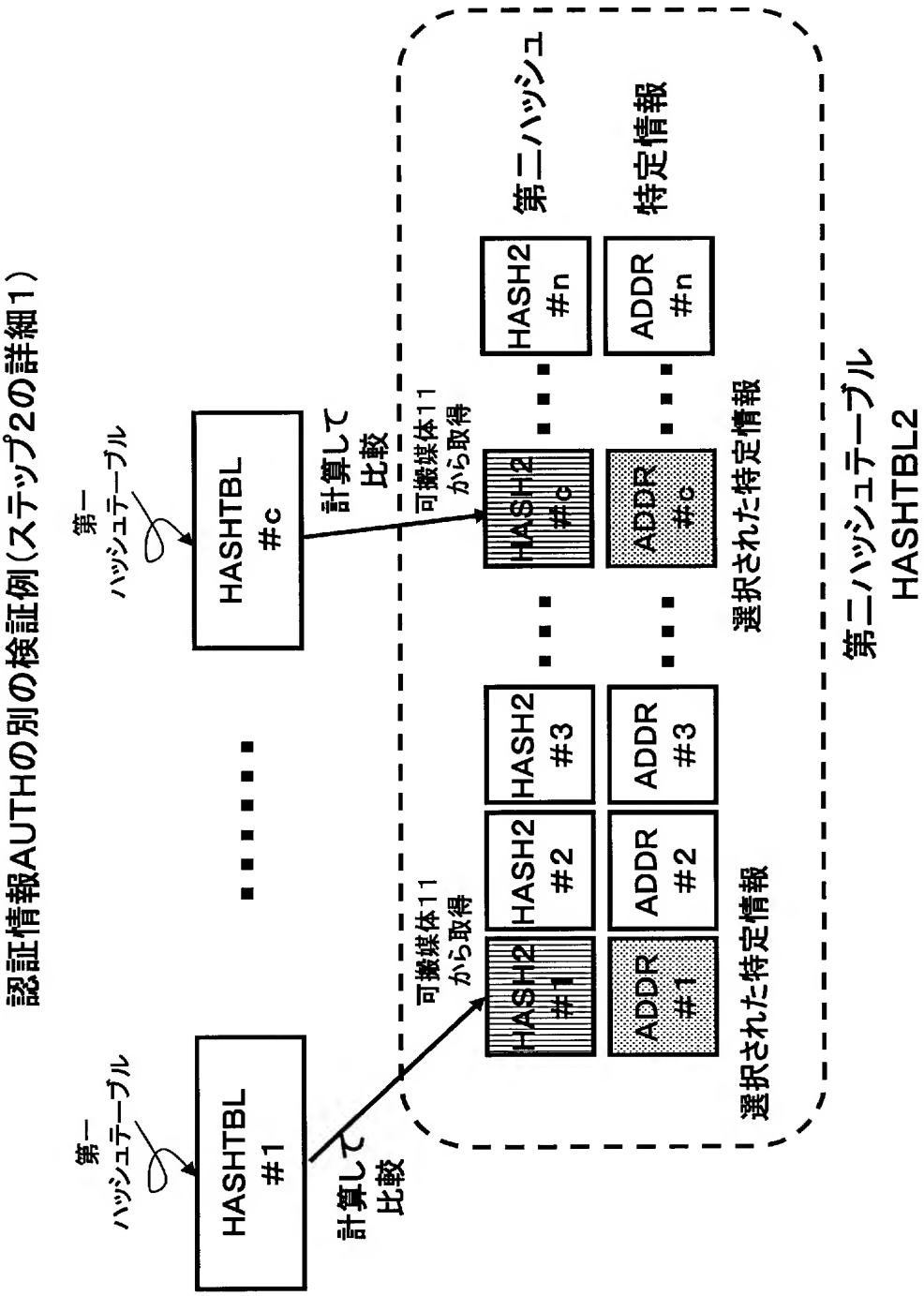
認証情報AUTHの別の検証例（ステップ1）



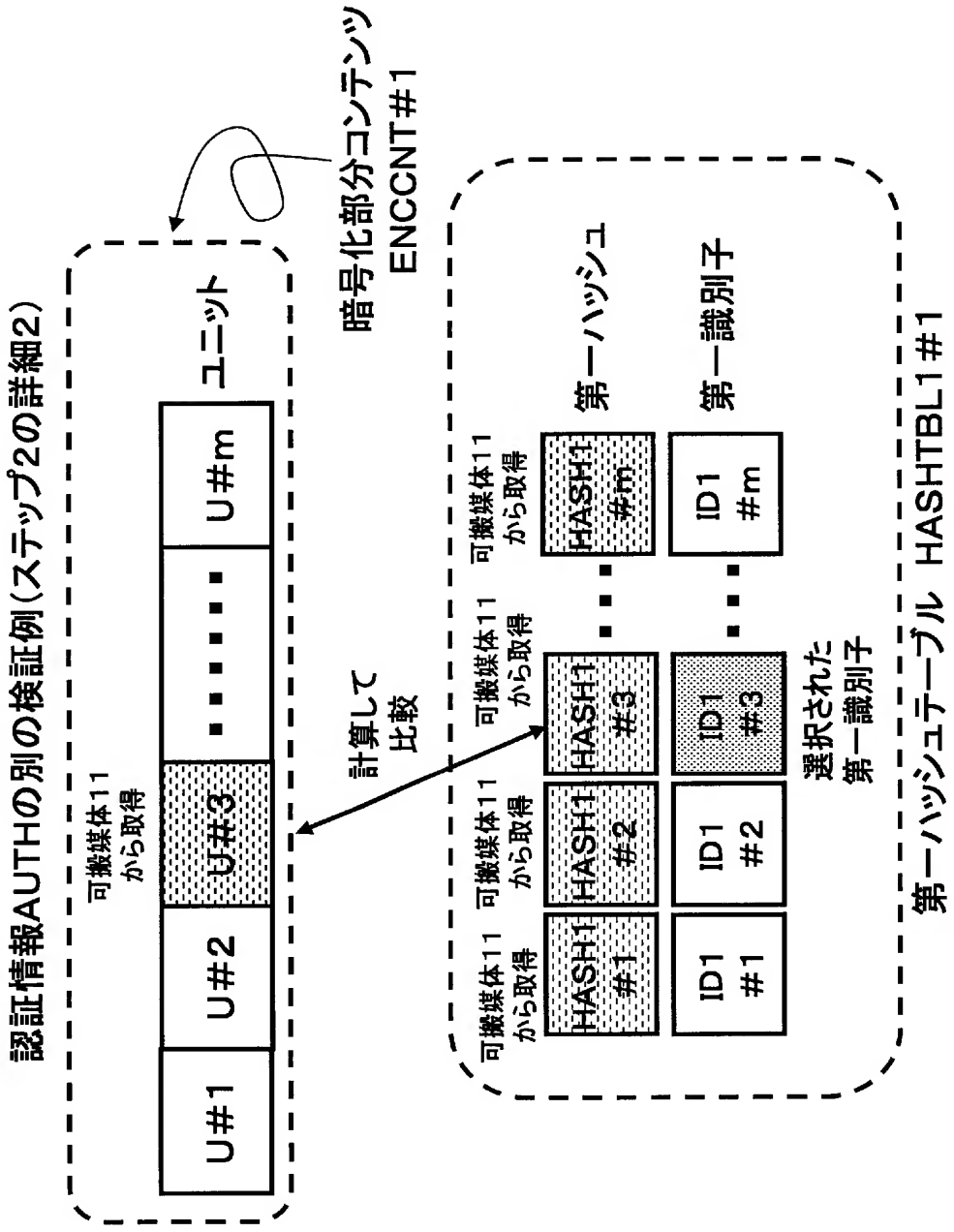
【図３４】


認証情報AUTHの別の検証例(ステップ2)
選択された特定情報
特定情報
ADDR#1
暗号化部分コンテンツ
ENCCNT#1
比較
第一ハッシュテーブル
HASHTBL1#1
選択された特定情報
特定情報
ADDR#c
暗号化部分コンテンツ
ENCCNT#c
比較
第一ハッシュテーブル
HASHTBL1#c

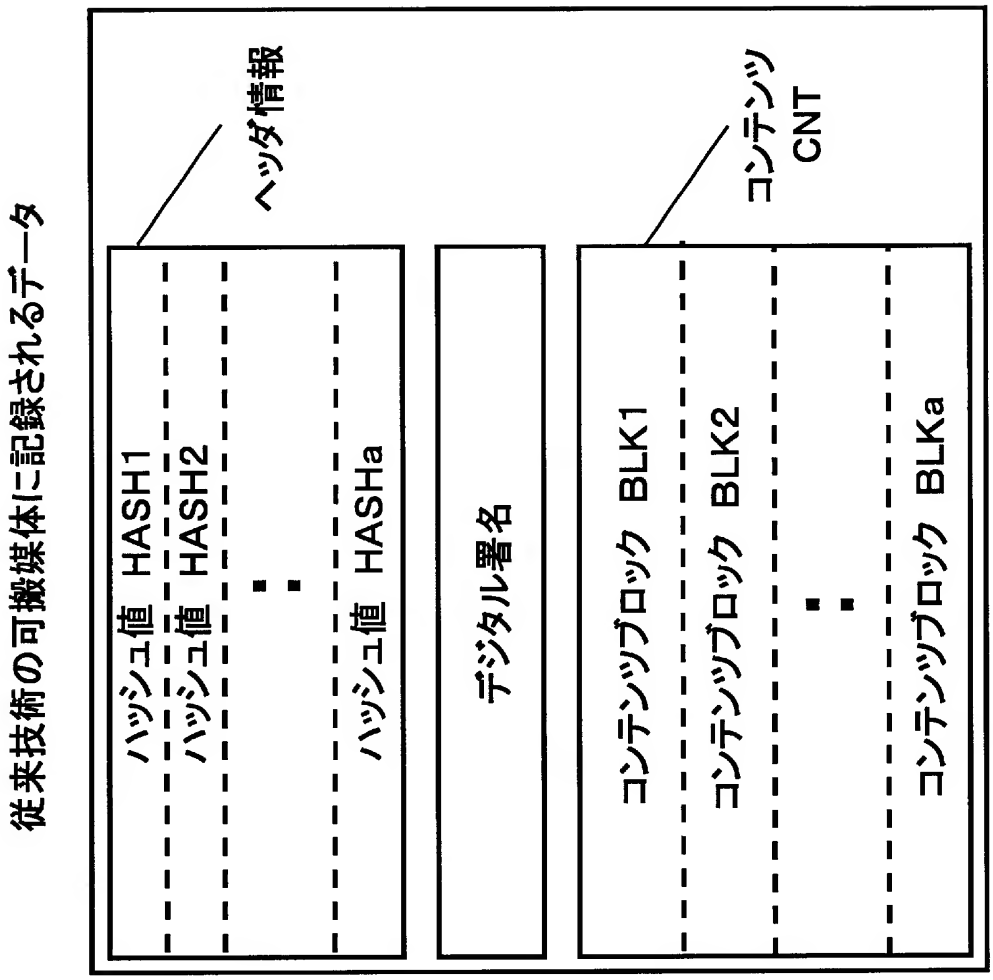
【図３５】


認証情報AUTHの別の検証例（ステップ2の詳細1）
第一
ハッシュテーブル
HASHTBL
#1
HASHTBL
#c
計算して
比較
可搬媒体11
から取得
HASH2
#1
HASH2
#2
HASH2
#3
HASH2
#c
HASH2
#n
ADDR
#1
ADDR
#2
ADDR
#3
ADDR
#c
ADDR
#n
選択された特定情報
第二ハッシュ
特定情報
第二ハッシュテーブル
HASHTBL2

【図３６】


認証情報AUTHの別の検証例(ステップ2の詳細2)
可搬媒体11から取得
U#1
U#2
U#3
U#m
ユニット
暗号化部分コンテンツ
ENCCNT#1
計算して比較
可搬媒体11から取得
HASH1 #1
HASH1 #2
HASH1 #3
HASH1 #m
第一ハッシュ
ID1 #1
ID1 #2
ID1 #3
ID1 #m
第一識別子
選択された第一識別子
第一ハッシュテーブル HASHTBL1#1

【図３７】


従来技術の可搬媒体に記録されるデータ
ヘッダ情報
ハッシュ値 HASH1
ハッシュ値 HASH2
ハッシュ値 HASHa
デジタル署名
コンテンツ CNT
コンテンツブロック BLK1
コンテンツブロック BLK2
コンテンツブロック BLKa

【書類名】要約書
【要約】
【課題】　実行装置において不正コンテンツかどうか検知することが出来なかった。
【解決手段】　配布センタ１０が、コンテンツＣＮＴとともに、そのコンテンツの領域を特定する配布データ領域特定情報と、配布データ領域特定情報を含む検証対象データに対する認証情報ＡＵＴＨを可搬媒体１１に記録し、実行装置１２では、コンテンツＣＮＴの実行、再生開始前に、認証情報ＡＵＴＨが正規の認証情報であるか検証し、検証結果が正当な場合にのみ、配布データ領域特定情報を基に配布データを特定し、配布データのみを実行する。
【選択図】　図１

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社